Spacy HITs statistics about NIS 2 directive

Legend

Name	Acronym
Member State	MS
National Cybsersecurity Strategy	NCS
Competent Authority	CA
Commission	Co
Point of Contact	POC
CSIRT	C
ENISA	E
Cooperation Group	CG
The European External Action Service	EEAS
CN	CSIRTs Network
Eu-Cyclone	EuC

Methodology

Article 7

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	MS	MS	✔	adopt	adopt	✔	**N7.1.1**	**S7.1.1**	✔
1.2	NCS	NCS	✔	include	include	✔	-	-	-
1.2.a	-	-	-	-	-	-	**N7.1.2.a**	**S7.1.2.a**	✔
1.2.b	-	-	-	-	-	-	**N7.1.2.b**	**S7.1.2.b**	✔
1.2.c	-	-	-	-	-	-	**N7.1.2.c**	**S7.1.2.c**	✔
1.2.d	-	-	-	-	-	-	**N7.1.2.d**	**S7.1.2.d**	✔
1.2.e	-	-	-	-	-	-	**N7.1.2.e**	**S7.1.2.e**	✔
1.2.f	-	-	-	-	-	-	**N7.1.2.f**	**S7.1.2.f**	✔
1.2.g	-	-	-	-	-	-	**N7.1.2.g**	**S7.1.2.g**	✔
1.2.h	-	-	-	-	-	-	**N7.1.2.h**	**S7.1.2.h**	✔
2.1	MS	MS	✔	adopt	adopt	✔	-	-	-
2.1.a	-	-	-	-	-	-	**N7.2.1.a**	**S7.2.1.a**	✔
2.1.b	-	-	-	-	-	-	**N7.2.1.b**	**S7.2.1.b**	✔
2.1.c	-	-	-	-	-	-	**N7.2.1.c**	**S7.2.1.c**	✔
2.1.d	-	-	-	-	-	-	**N7.2.1.d**	**S7.2.1.d**	✔
2.1.e	-	-	-	-	-	-	**N7.2.1.e**	**S7.2.1.e**	✔
2.1.f	-	-	-	-	-	-	**N7.2.1.f**	**S7.2.1.f**	✔
2.1.g	-	-	-	-	-	-	**N7.2.1.g**	**S7.2.1.g**	✔
2.1.h	-	-	-	-	-	-	**N7.2.1.h**	**S7.2.1.h**	✔
2.1.i	-	-	-	-	-	-	**N7.2.1.i**	**S7.2.1.i**	✔
2.1.j	-	-	-	-	-	-	**N7.2.1.j**	**S7.2.1.j**	✔
3.1	MS	MS	✔	notify	notify	✔	**N7.3.1**	**S7.3.1**	✔
3.2	MS	MS	✔	exclude	exclude	✔	**N7.3.2**	**S7.3.2**	✔
4.1	MS	MS	✔	assess	assess	✔	**N7.4.1**	**S7.4.1**	❙
4.2	ENISA	ENISA	✔	assist	assist	✔	**N7.4.2**	**S7.4.2**	❙
	Sub-HIT % = 100 %			**Sub-HIT % = 100 %**			**Obj-HIT % = 91.6 %**		

Article 8

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	MS	MS	✔	designate	designate	✔	**N8.1**	**S8.1**	❙
2	CA	CA	✔	monitor	referred	✘	**N8.2**	**S8.2**	❙
3.1	MS	MS	✔	designate	designate	✔	**N8.3.1**	**S8.3.1**	❙
3.2	CA	CA	✔	be	be	✔	**N8.3.2**	**S8.3.2**	✘
4	POC	POC	✔	exercise	exercise	✔	**N8.4**	**S8.4**	❙
5	MS	MS	✔	ensure	ensure	✔	**N8.5**	**S8.5**	✔
6.1	MS	MS	✔	notify	notify	✔	**N8.6.1**	**S8.6.1**	❙
6.2	MS	MS	✔	make	make	✔	**N8.6.2**	**S8.6.2**	✔
6.3	Co	Co	✔	make	make	✔	**N8.6.3**	**S8.6.3**	✔
	Sub-HIT % = 100 %			**Sub-HIT % = 88.8 %**			**Obj-HIT % = 61.1 %**		

Article 9

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	MS	MS	✔	designate	designate	✔	**N9.1.1**	**S9.1.1**	✔
1.2	MS	MS	✔	ensure	ensure	✔	**N9.1.2**	**S9.1.2**	❙
1.3	MS	MS	✔	ensure	ensure	✔	**N9.1.3**	**S9.1.3**	✔
2	MS	MS	✔	indicate	indicate	✔	**N9.2**	**S9.2**	✔
3	MS	MS	✔	identify	identify	✔	**N9.3**	**S9.3**	✔
4.1	MS	MS	✔	adopt	adopt	✔	**N9.4.1**	**S9.4.1**	✔
4.2	Plan	Plan	✔	lay	lay	✔	-	-	-
4.2.a	-	-	-	-	-	-	**N9.4.2.a**	**S9.4.2.a**	✘
4.2.b	-	-	-	-	-	-	**N9.4.2.b**	**S9.4.2.b**	✘
4.2.c	-	-	-	-	-	-	**N9.4.2.c**	**S9.4.2.c**	✘
4.2.d	-	-	-	-	-	-	**N9.4.2.d**	**S9.4.2.d**	✘
4.2.e	-	-	-	-	-	-	**N9.4.2.e**	**S9.4.2.e**	✘
4.2.f	-	-	-	-	-	-	**N9.4.2.f**	**S9.4.2.f**	✘
5.1	MS	MS	✔	notify	notify	✔	**N9.5.1**	**S9.5.1**	✔
5.2	MS	MS	✔	submit	submit	✔	**N9.5.2**	**S9.5.2**	✘
5.3	MS	MS	✔	exclude	exclude	✔	**N9.5.3**	**S9.5.3**	✘
	Sub-HIT % = 100 %			**Sub-HIT % = 100 %**			**Obj-HIT % = 43.3 %**		

Article 10

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	MS	MS	✔	designate	designate	✔	**N10.1.1**	**S10.1.1**	✔
1.2	C	C	✔	P - designated or established	designated	❙	**N10.1.2**	**S10.1.2**	✘
1.3	MS	MS	✔	cover, comply, ...	cover	❙	**N10.1.3**	**S10.1.3**	✘
2	MS	MS	✔	ensure	ensure	✔	**N10.2**	**S10.2**	✔
3.1	MS	MS	✔	ensure	ensure	✔	**N10.3.1**	**S10.3.1**	✔
3.2	MS	MS	✔	ensure	ensure	✔	**N10.3.2**	**S10.3.2**	✔
4	C	C	✔	cooperate	cooperate	✔	**N10.4**	**S10.4**	❙
5	C	C	✔	participate	participate	✔	**N10.5**	**S10.5**	✘
6	MS	MS	✔	ensure	ensure	✔	**N10.6**	**S10.6**	✔
7.1	C	C	✔	establish	establish	✔	**N10.7.1**	**S10.7.1**	✔
7.2	MS	MS	✔	facilitate	facilitate	✔	**N10.7.2**	**S10.7.2**	✔
7.3	C	C	✔	exchange	exchange	✔	**N10.7.3**	**S10.7.3**	✔
8	C	C	✔	cooperate	cooperate	✔	**N10.8**	**S10.8**	✘
9	MS	MS	✔	notify	notify	✔	**N10.9**	**S10.9**	✘
10	MS	MS	✔	request	request	✔	**N10.10**	**S10.10**	❙
	Sub-HIT % = 100 %			**Sub-HIT % = 93.3 %**			**Obj-HIT % = 60 %**		

Article 11

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	-	-	-	-	-	-	-	-	-
1.a	C	C	✔	ensure	ensure	✔	**N11.1.2.a**	**S11.1.2.a**	❙
1.b	C Premises	C premises	❙	located	located	✔	**N11.1.2.b**	**S11.1.2.b**	✘
1.c	C	C	✔	equipped	equipped	✔	**N11.1.2.c**	**S11.1.2.c**	✘
1.d	C	C	✔	ensure	ensure	✔	**N11.1.2.f**	**S11.1.2.f**	✔
1.e	C	C	✔	staffed	ensure — ensure	✔	**N11.1.2.e**	**S11.1.2.e**	✘
1.f	C	C	✔	equipped	equipped	✔	**N11.1.2.f**	**S11.1.2.f**	✘
2.1	MS	MS	✔	ensure	ensure	✔	**N11.2.1**	**S11.2.1**	✔
2.2	MS	MS	✔	ensure	ensure	✔	**N11.2.2**	**S11.2.2**	✔
3	-	-	-	-	-	-	-	-	-
4	MS	MS	✔	establish	establish	✔	**N11.4.1**	**S11.4.1**	✔
5.1	C	C	✔	promote	facilitate	✘	-	-	-
5.1.a	-	-	-	-	-	-	**N11.5.1.a**	**S11.5.1.a**	✘
5.1.b	-	-	-	-	-	-	**N11.5.1.b**	**S11.5.1.b**	✘
5.1.c	-	-	-	-	-	-	**N11.5.1.c**	**S11.5.1.c**	✘
	Sub-HIT % = 95 %			**Sub-HIT % = 90 %**			**Obj-HIT % = 45 %**		

Article 12

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	MS	MS	✔	designate	designate	✔	**N12.1.1**	**S12.1.1**	✔
1.2	C	C	✔	act	designated	✘	**N12.1.2**	**S12.1.2**	✘
1.3	C	C	✔	act	designated	✘	-	-	-
1.3.a	-	-	-	-	-	-	**N12.1.3.a**	**S12.1.3.a**	✔
1.3.b	-	-	-	-	-	-	**N12.1.3.b**	**S12.1.3.b**	✔
1.3.c	-	-	-	-	-	-	**N12.1.3.c**	**N12.1.3.c**	✔
2.1	E	E	✔	develop	develop	✔	**N12.2.1**	**S12.2.1**	✘
2.2	E	E	✔	establish and maintain	establish	❙	**N12.2.2**	**S12.2.2**	✘
2.3	All stake.	all stake.	✔	be provided	provided	❙	??	??	✔
2.4	That db	that db	✔	include	include	✔	-	-	-
2.4.a	-	-	-	-	-	-	??	??	✔
2.4.b	-	-	-	-	-	-	??	??	✔
2.4.c	-	-	-	-	-	-	??	??	✘
	Sub-HIT % = 100 %			**Sub-HIT % = 57.14 %**			**Obj-HIT % = 58.3 %**		

Article 13

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	C, PoC	they	✘	cooperate	are	✘	**N13.1.1**	**S13.1.1**	✘
2	MS	MS	✔	ensure	ensure	✔	**N13.2.1**	**S13.2.1**	✔
3	MS	MS	✔	ensure	ensure	✔	**N13.3.1**	**S13.3.1**	✔
4	MS	MS	✔	ensure	ensure	✔	**N13.4.1**	**S13.4.1**	❙
5.1	MS	MS	✔	ensure	ensure	✔	**N13.5.1**	**S13.5.1**	✔
5.2	MS	MS	✔	ensure	ensure	✔	**N13.5.2**	**S13.5.2**	✘
6	MS	MS	✔	simplify	simplify	✔	**N13.6.1**	**S13.6.1**	✘
	Sub-HIT % = 85.7 %			**Sub-HIT % = 85.7 %**			**Obj-HIT % = 50 %**		

Article 14

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	-	-	-	P	P	-	**N14.1.1**	**S14.1.1**	✘
2	CG	CG	✔	carry	carry	✔	**N14.2.1**	**S14.2.1**	✔
3.1	CG	CG	✔	P - composed	P - composed	✔	**N14.3.1**	**S14.3.1**	✘
3.2	ESA	ESA	❙	participate	participate	✔	**N14.3.2**	**S14.3.2**	✘
3.3	ESA - CA	ESA	❙	participate	participate	✔	**N14.3.3**	**S14.3.3**	✘
4.1	CG	CG	✔	have	have	✔	-	-	-
4.1.X	-	-	-	-	-	-	-	-	-
5	MS	MS	✔	ensure	ensure	✔	**N14.5.1**	**S14.5.1**	✔
6	CG	CG	✔	request	request	✔	**N14.6.1**	**S14.6.1**	✔
7	CG	CG	✔	establish	establish	✔	**N14.7.1**	**S14.7.1**	✔
8	Co	Co	✔	adopt	adopt	✔	**N14.8.1**	**S14.8.1**	✔
9	CG	CG	✔	meet	meet	✔	**N14.9.1**	**S14.9.1**	✘
	Sub-HIT % = 90%			**Sub-HIT % = 100 %**			**Obj-HIT % = 50 %**		

Article 15

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	C Network	-	✔	P - established	-	✘	**N15.1.1**	**S15.1.1**	-
2.1	C Network	C Network	✔	P - composed	P - composed	✔	**N15.2.1**	**S15.2.1**	✘
2.2	Co	Co	✔	participate	participate	✔	**N15.2.2**	**S15.2.2**	✘
2.3	E	E	✔	provide - provide	provide	✔	**N15.2.3**	**S15.2.3**	❙
3.1	C Network	C Network	✔	have	have	✔	-	-	-
3.1.X	-	-	-	-	-	-	-	-	-
4.1	CN	CN	✔	assess	referred	✘	**N15.4.1**	**S15.4.1**	✔
4.2	Report	Report	✔	draw	draw	✔	**N15.4.2**	**S15.4.2**	✔
4.3	Report	Report	✔	P - submitted	submitted	✔	**N15.4.3**	**S15.4.3**	✘
5	CN	CN	✔	adopt	adopt	✔	**N15.5.1**	**S15.5.1**	✔
6	CN - EuC	CN	❙	agree	agree	✔	**N15.6.1**	**S15.6.1**	✘
	Sub-HIT % = 95 %			**Sub-HIT % = 80 %**			**Obj-HIT % = 43.8%**		

Article 16

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	EuC	EuC	✔	support	support	✔	**N16.1.1**	**S16.1.1**	✔
2.1	EuC	EuC	✔	composed	composed	✔	**N16.2.1**	**S16.2.1**	✘
2.2	Co	Co	✔	participate	participate	✔	**N16.2.2**	**S16.2.2**	✘
3.1	C Network	C Network	✔	have	have	✔	-	-	-
3.1.a	-	-	-	-	-	-	**N16.3.1.a**	**S16.3.1.a**	✔
3.1.b	-	-	-	-	-	-	**N16.3.1.b**	**S16.3.1.b**	✔
3.1.c	-	-	-	-	-	-	**N16.3.1.c**	**S16.3.1.c**	✔
3.1.d	-	-	-	-	-	-	**N16.3.1.d**	**S16.3.1.d**	✔
3.1.e	-	-	-	-	-	-	**N16.3.1.e**	**S16.3.1.e**	✔
4	EuC	EuC	✔	adopt	adopt	✔	**N16.4.1**	**S16.4.1**	✔
5	EuC	EuC	✔	report	focusing	✘	**N16.5.1**	**S16.5.1**	✘
6	EuC	EuC	✔	cooperate	cooperate	✔	**N16.6.1**	**S16.6.1**	✘
7	EuC	EuC	✔	submit	submit	✔	**N16.7.1**	**S16.7.1**	✔
	Sub-HIT % = 100 %			**Sub-HIT % = 87.5 %**			**Obj-HIT % = 66.6 %**		

Article 17

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
-	-	-	-	-	-	-	-	-	-
	Sub-HIT % = %			**Sub-HIT % = %**			**Obj-HIT % = %**		

Article 18

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	E	E	✔	adopt, submit	present	✘	**N18.1.1**	**S18.1.1**	✔
1.2	The Report	The Report	✔	be made	NONE	✘	-	-	-
1.2.X	-	-	-	-	-	-	-	-	✘
2	The report	The report	✔	include	include	✔	**N18.2.1**	**S18.2.1**	✔
3	E	E	✔	develop	develop	✔	**N18.3.1**	**S18.3.1**	✔
	Sub-HIT % = 100 %			**Sub-HIT % = 50 %**			**Obj-HIT % = 75 %**		

Article 19

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	CG	CG	✔	establish	establish	✔	**N19.1.1**	**S19.1.1**	✘
1.2	The peer reviews	The peer reviews	✔	P - be carried	carried	✔	**N19.1.2**	**S19.1.2**	✘
1.3	Cybersec Experts	Cybersec Experts	✔	P - be designated	designated	✔	**N19.1.3**	**S19.1.3**	✘
2.1	The methodology	The methodology	✔	include	referred	✘	**N19.2.1**	**S19.2.1**	✔
2.2	The Commission and E	The Commission and E	✔	participate	participate	✔	**N19.2.2**	**S19.2.2**	✘
3	MS	MS	✔	identify	identify	✔	**N19.3.1**	**S19.3.1**	❙
4	MS	MS	✔	notify	notify	✔	**N19.4.1**	**S19.4.1**	❙
5.1	MS	MS	✔	carry,provide	provide	❙	**N19.5.1**	**S19.5.1**	❙
5.2	CG	CG	✔	lay	lay	✔	**N19.5.2**	**S19.5.2**	✔
6.1	Peer Reviews	Peer Reviews	✔	entail	entail	✔	**N19.6.1**	**S19.6.1**	✔
6.2	MS	MS	✔	provide	provide	✔	**N19.6.2**	**S19.6.2**	✔
6.3	CG	CG	✔	develop	develop	✔	**N19.6.3**	**S19.6.3**	✔
6.4	-	-	-	-	-	-	-	-	-
6.5	Cybersecs Experts	Cybersecs Experts	✔	not disclose	disclose	✘	**N19.6.5**	**S19.6.5**	✔
7	The same aspects r. in a MS	The same aspects r. in a MS	✔	not be	be	✘	**N19.7.1**	**S19.7.1**	✘
8.1	MS	MS	✔	ensure	ensure	✔	**N19.8.1**	**S19.8.1**	✔
8.2	MS	review	✔	object	object	✔	**N19.8.2**	**S19.8.2**	?
9.1	Cybersecs Experts	Cybersecs Experts	✔	draft	draft	✔	**N19.9.1**	**S19.9.1**	✔
9.2	MS	MS	✔	provide	provide	✔	**N19.9.2**	**S19.9.2**	✔
9.3	The reports	The reports	✔	include	include	✔	**N19.9.3**	**S19.9.3**	✔
9.4	The reports	The reports	✔	P - submitted	submitted	✔	**N19.9.4**	**S19.9.4**	✘
9.5	MS	MS	✔	decide	decide	✔	**N19.5.1**	**S19.5.1**	✘
	Sub-HIT % = 100 %			**Sub-HIT % = 83.3 %**			**Obj-HIT % = 57.5 %**		

Article 20

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	MS	MS	❙	ensure	ensure	✔	**N20.1.1**	**S20.1.1**	✔
2	MS	MS	✔	ensure,encourage	ensure	❙	**S20.2.1**	**S20.2.1**	✔
	Sub-HIT % = 75 %			**Sub-HIT % = 75 %**			**Obj-HIT % = 100 %**		

Article 21

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	MS	MS,...	❙	ensure	ensure	✔	**N21.1.1**	**S21.1.1**	✘
2	-	-	-	-	-	-	-	-	-
3.1	MS	MS	✔	ensure	ensure	✔	??	??	✔
3.2	MS	MS	✔	ensure	ensure	✔	??	??	✘
4	MS	MS	✔	ensure	ensure	✘	??	??	✔
5	MS	MS	✔	adopt	adopt	✘	??	??	✔
	Sub-HIT % = 90 %			**Sub-HIT % = 60 %**			**Obj-HIT % = 60 %**		

Article 22

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	CG	CG	✔	carry	carry	✔	**N22.1.1**	**S22.1.1**	❙
2	Commission	Commission	✔	identify	identify	✔	**N22.2.1**	**S22.2.1**	❙
	Sub-HIT % = 100 %			**Sub-HIT % = 100 %**			**Obj-HIT % = 50 %**		

Article 23

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	MS	MS	✔	ensure	ensure	✔	**N23.1.1**	**S23.1.1**	✔
1.2	Entities concerned	Entities Concerned	✔	ensure	ensure	✔	**N23.1.2**	**S23.1.2**	✔
1.3	MS	MS	✔	ensure	ensure	✔	**N23.1.3**	**S23.1.3**	✔
1.4	Mere ... notification	Mere ... notification	✔	not subject	subject	✘	**N23.1.4**	**S23.1.4**	✔
2.1	MS	MS	✔	ensure	ensure	✔	**N23.2.1**	**S23.2.1**	✔
2.2	The entities	The entities	✔	inform	inform	✔	**N23.2.2**	**S23.2.2**	✔
3.1	An incident	An incident	✔	P - be considered	be considered	✔	-	-	-
3.1.a	-	-	-	-	-	-	**N23.3.1.a**	**S23.3.1.a**	✔
3.1.b	-	-	-	-	-	-	**N23.3.1.b**	**S23.3.1.b**	✔
4	MS	MS	✔	ensure	ensure	✔	**??**	**??**	✔
4.1.a	-	-	-	-	-	-	**??**	**??**	✔
4.1.b	-	-	-	-	-	-	**N23.4.1.a**	**S23.3.1.a**	✔
4.1.c	-	-	-	-	-	-	**??**	**??**	✔
4.1.d	-	-	-	-	-	-	**??**	**??**	✔
4.1.e	-	-	-	-	-	-	**??**	**??**	✔
5.1	C	C	✔	provide	provide	✔	**N23.5.1**	**S23.5.1**	✔
5.2	NR	NR	NR	NR	NR	NR	NR	NR	NR
5.3	C	C	✔	provide	provide	✔	**N23.5.3**	**S23.5.3**	❙
5.4	C	C	✔	provide	provide	✔	**N23.5.4**	**S23.5.4**	✔
6.1	MS	MS	✔	inform	inform	✔	**N23.6.1**	**S23.6.1**	✔
6.2	Such inf.	Such inf.	✔	include	include	✔	**N23.6.2**	**S23.6.2**	✔
6.3	C, CA, POC	C	❙	preserve	NONE	✘	**N23.6.3**	**S23.6.3**	✔
7	C	Public awareness	✘	inform	NONE	✘	**N23.7.1**	**S23.7.1**	✘
8	POC	POC	✔	forward	NONE	✘	**N23.8.1**	**S23.8.1**	✘
9.1	POC	POC	✔	submit	submit	✔	**N23.9.1**	**S23.9.1**	✔
9.2	E	E	✔	contribute	contribute	✔	**N23.9.2**	**S23.9.2**	✔
9.3	E	E	✔	inform	inform	✔	**N23.9.3**	**S23.9.3**	✔
10	C	C	✔	provide	provide	✔	**N23.10.1**	**S23.10.1**	✘
11	Commission	Commission	✔	adopt	adopt	✔	**N23.11.1**	**S23.11.1**	✘
	Sub-HIT % = 92.8 %			**Sub-HIT % = 80.9 %**			**Obj-HIT % = 83.3 %**		

Article 24

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	MS	MS	✔	require	require	✔	**N24.1.1**	**S24.1.1**	❙
1.2	MS	MS	✔	encourage	encourage	✔	**N24.1.2**	**S24.1.2**	❙
2.1	Commission	Commission	✔	P - is empowered	empowered	✔	**N24.2.1**	**S24.2.1**	✘
2.2	Those ... acts	Those ... acts	✔	P - be adopted	adopted	✔	**N24.2.2**	**S24.2.2**	✔
3	Commission	NONE	✘	request	NONE	✘	**N24.3.1**	**S24.3.1**	✘
	Sub-HIT % = 80 %			**Sub-HIT % = 80 %**			**Obj-HIT % = 40 %**		

Article 25

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	MS	MS	✔	encourage	encourage	✔	**N25.1.1**	**S25.1.1**	✔
2	E	E	✔	draw	draw	✔	**N25.2.1**	**S25.2.1**	✘
	Sub-HIT % = 100 %			**Sub-HIT % = 100 %**			**Obj-HIT % = 50 %**		

Article 26

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	Entities falling...	Entities falling...	✔	be considered	be considered	✔	-	-	-
1.1.a	-	-	-	-	-	-	??	??	✔
1.1.b	-	-	-	-	-	-	??	??	✘
1.1.c	-	-	-	-	-	-	??	??	✘
2 to 5	NR	NR	NR	NR	NR	NR	NR	NR	NR
	Sub-HIT % = 100 %			**Sub-HIT % = 100 %**			**Obj-HIT % = 33.3%**		

Article 27

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	E	E	✔	create, maintain	create	❙	**N27.1.1**	**S27.1.1**	✘
1.2	E	E	✔	allow	allow	✔	**N27.1.2**	**S27.1.2**	❙
2.1	MS	MS	✔	require	require	✔	-	-	-
2.1.a	-	-	-	-	-	-	**N27.2.1.a**	**S27.2.1.a**	✔
2.1.b	-	-	-	-	-	-	**N27.2.1.b**	**S27.2.1.b**	✔
2.1.c	-	-	-	-	-	-	**N27.2.1.c**	**S27.2.1.c**	✔
2.1.d	-	-	-	-	-	-	**N27.2.1.d**	**S27.2.1.d**	✔
2.1.e	-	-	-	-	-	-	**N27.2.1.e**	**S27.2.1.e**	✔
2.1.f	-	-	-	-	-	-	**N27.2.1.f**	**S27.2.1.f**	✔
3	MS	MS	✔	ensure	ensure	✔	**N27.3.1**	**S27.1.1**	✔
4	NR	NR	NR	NR	NR	NR	NR	NR	NR
5	NR	NR	NR	NR	NR	NR	NR	NR	NR
	Sub-HIT % = 100 %			**Sub-HIT % = 75 %**			**Obj-HIT % = 83.3 %**		

Article 28

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	MS	MS	✔	require	require	✔	**N28.1.1**	**S28.1.1**	✔
2.1	MS	MS	✔	require	require	✔	**N28.2.1**	**S28.2.1**	✔
2.2	Such information	Such information	✔	include	include	✔	-	-	-
2.2.a	-	-	-	-	-	-	**N28.2.2.a**	**S28.2.2.a**	✔
2.2.b	-	-	-	-	-	-	**N28.2.2.b**	**S28.2.2.b**	✔
2.2.c	-	-	-	-	-	-	**N28.2.2.c**	**S28.2.2.c**	✔
2.2.d	-	-	-	-	-	-	**N28.2.2.d**	**S28.2.2.d**	✔
3.1	MS	MS	✔	require	require	✔	**N28.3.1**	**S28.3.1**	✔
3.2	MS	MS	✔	require	require	✔	**N28.3.2**	**S28.3.2**	✔
4	MS	MS	✔	require	require	✔	**N28.4.1**	**S28.4.1**	✔
5.1	MS	MS	✔	require	require	✔	**N28.5.1**	**S28.5.1**	✔
5.1	MS	MS	✔	require	require	✔	**N28.5.1**	**S28.5.1**	✔
5.2	MS	MS	✔	require	require	✔	**N28.5.2**	**S28.5.2**	✔
5.3	MS	MS	✔	require	require	✔	**N28.5.3**	**S28.5.3**	✘
6.1	Compliance	Compliance	✔	not result	result	✘	**N28.6.1**	**S28.6.1**	✘
6.2	MS	MS	✔	require	require	✔	**N28.6.2**	**S28.6.2**	✔
	Sub-HIT % = 100 %			**Sub-HIT % = 91.6 %**			**Obj-HIT % = 86.6 %**		

Article 29

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	MS	MS	✔	ensure	ensure	✔	-	-	-
1.1.a	-	-	-	-	-	-	**N29.1.a**	**S29.1.a**	✘
1.1.b	-	-	-	-	-	-	**N29.1.b**	??	✘
2.1	MS	MS	✔	ensure	ensure	✔	**N29.2.1**	**S29.2.1**	✔
2.2	Such exchange	Such exchange	✔	P - implemented	implemented	✔	**N29.2.2**	**S29.2.2**	✘
3.1	MS	MS	✔	facilitate	facilitate	✔	**N29.3.1**	**S29.3.1**	✔
3.2	Such arrangements	Such arrangements	✔	specify	specify	✔	**N29.3.2**	**S29.3.2**	✔
3.3	MS	MS	✔	impose	impose	✔	**N29.3.3**	**S29.3.3**	✔
4	MS	MS	✔	ensure	ensure	✔	**N29.4.1**	**S29.4.1**	✔
5	E	E	✔	provide	provide	✔	**N29.5.1**	**S29.5.1**	✔
	Sub-HIT % = 100 %			**Sub-HIT % = 100 %**			**Obj-HIT % = 66.7 %**		

Article 30

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	MS	MS	✔	ensure	ensure	✔	-	-	-
1.a	-	-	-	-	-	-	**N30.1.a**	**S30.1.a**	✔
1.b	-	-	-	-	-	-	**N30.1.b**	**S30.1.b**	✔
2.1	MS	MS	✔	process	process	✔	**N30.2.1**	**S30.2.1**	✔
2.2	MS	MS	✔	prioritise	prioritise	✔	**N30.2.2**	**S30.2.2**	✔
	Sub-HIT % = 100 %			**Sub-HIT % = 100 %**			**Obj-HIT % = 100%**		

Article 31

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	MS	MS	✔	ensure	ensure	✔	**N31.1.1**	**S31.1.1**	✔
2.1	MS	MS	✔	allow	allow	✔	**N31.2.1**	**S31.2.1**	✔
2.2	Such prioritisation	Such prioritisation	✔	P - be based	be based	✔	**N31.2.2**	**S31.2.2**	✘
2.3	Comp. Auth.	Comp. Auth.	✔	establish	exercising	✘	**N31.2.3**	**S31.2.3**	✘
3	Comp. Auth.	Comp. Auth.	✔	work	work	✔	**N31.3.1**	**S31.3.1**	✘
4.1	MS	MS	✔	ensure	ensure	✔	**N31.4.1**	**S31.4.1**	✔
4.2	MS	MS	✔	decide	decide	✔	**N31.4.2**	**S31.4.2**	✘
	Sub-HIT % = 100 %			**Sub-HIT % = 85.7 %**			**Obj-HIT % = 42.85 %**		

Article 32

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	MS	MS	✔	ensure	ensure	✔	**N32.1.1**	**S32.1.1**	✔
2.1	MS	MS	✔	ensure	ensure	✔	-	-	-
2.1.a	-	-	-	-	-	-	**N32.2.a**	**S32.2.a**	✔
2.1.b	-	-	-	-	-	-	**N32.2.b**	**S32.2.b**	✔
2.1.c	-	-	-	-	-	-	**N32.2.c**	**S32.2.c**	✔
2.1.d	-	-	-	-	-	-	**N32.2.d**	**S32.2.d**	✔
2.1.e	-	-	-	-	-	-	**N32.2.e**	**S32.2.e**	✔
2.1.f	-	-	-	-	-	-	**N32.2.f**	**S32.2.f**	✔
2.1.g	-	-	-	-	-	-	**N32.2.g**	**S32.2.g**	✔
3	Comp. Auth.	Comp. Auth.	✔	state	exercising	✘	**N32.3.1**	**S32.3.1**	✘
4.1	MS	MS	✔	ensure	ensure	✔	-	-	-
4.1.a	-	-	-	-	-	-	**N32.4.1.a**	**S32.4.1.a**	✔
4.1.b	-	-	-	-	-	-	**N32.4.1.b**	**S32.4.1.b**	✔
4.1.c	-	-	-	-	-	-	**N32.4.1.c**	**S32.4.1.c**	✔
4.1.d	-	-	-	-	-	-	**N32.4.1.d**	**S32.4.1.d**	✔
4.1.e	-	-	-	-	-	-	**N32.4.1.e**	**S32.4.1.e**	✔
4.1.f	-	-	-	-	-	-	**N32.4.1.f**	**S32.4.1.f**	✔
4.1.g	-	-	-	-	-	-	**N32.4.1.g**	**S32.4.1.g**	✔
4.1.h	-	-	-	-	-	-	**N32.4.1.h**	**S32.4.1.h**	✔
4.1.i	-	-	-	-	-	-	**N32.4.1.i**	**S32.4.1.i**	✔
5.1	MS	MS	✔	ensure	are	✘	**N32.5.1**	**S32.5.1**	✘
5.2	MS	MS	✔	ensure	are	✘	-	-	-
5.2.a	-	-	-	-	-	-	**N32.5.2.a**	**S32.5.2.a**	✔
5.2.b	-	-	-	-	-	-	**N32.5.2.b**	**S32.5.2.b**	✔
6.1	MS	MS	✔	ensure	ensure	✔	**N32.6.1**	**S32.6.1**	❙
6.2	MS	MS	✔	ensure	ensure	✔	**N32.6.2**	**S32.6.2**	✔
7.1	Comp. Auth.	Comp. Auht.	✔	comply	taking	✘	-	-	-
7.1.a	-	-	-	-	-	-	**N32.7.1**	**S32.7.1**	✘
7.1.b	-	-	-	-	-	-	**N32.7.2**	**S32.7.2**	✘
7.1.c	-	-	-	-	-	-	**N32.7.3**	**S32.7.3**	✘
7.1.d	-	-	-	-	-	-	**N32.7.4**	**S32.7.4**	✘
7.1.e	-	-	-	-	-	-	**N32.7.5**	**S32.7.5**	✘
7.1.f	-	-	-	-	-	-	**N32.7.6**	**S32.7.6**	✘
7.1.g	-	-	-	-	-	-	**N32.7.7**	**S32.7.7**	✘
7.1.h	-	-	-	-	-	-	**N32.7.8**	**S32.7.8**	✘
8.1	Comp. Auth.	Comp. Auth.	✔	set	set	✔	**N32.8.1**	**S32.8.1**	✔
8.2	Comp. Auth.	Comp. Auth.	✔	notify	notify	✔	**N32.8.2**	**S32.8.2**	✔
8.3	They	They	✔	allow	allow	✔	**N32.8.3**	**S32.8.3**	✘
9.1	MS	MS	✔	ensure	ensure	✔	**N32.9.1**	**S32.9.1**	✔
9.2	Comp. Auth	Comp. Auth	✔	request	request	✔	**N32.9.2**	**S32.9.2**	✘
10.1	MS	MS	✔	ensure	ensure	✔	**N32.10.1**	**S32.10.1**	✔
10.2	MS	MS	✔	ensure	ensure	✔	**N32.10.2**	**S32.10.2**	✔
	Sub-HIT % = 100 %			**Sub-HIT % = 75 %**			**Obj-HIT % = 67.1 %**		

Article 33

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	MS	MS	✔	ensure	ensure	✔	**N33.1.1**	**S33.1.1**	✔
1.2	MS	MS	✔	ensure	ensure	✔	**N33.1.2**	**S33.1.2**	✔
2.1	MS	MS	✔	ensure	ensure	✔	-	-	-
2.1.a	-	-	-	-	-	-	**N33.2.a**	**S33.2.a**	✔
2.1.b	-	-	-	-	-	-	**N33.2.b**	**S33.2.b**	✔
2.1.c	-	-	-	-	-	-	**N33.2.c**	**S33.2.c**	✔
2.1.d	-	-	-	-	-	-	**N33.2.d**	**S33.2.d**	✔
2.1.e	-	-	-	-	-	-	**N33.2.e**	**S33.2.e**	✔
2.1.f	-	-	-	-	-	-	**N33.2.f**	**S33.2.f**	✔
3	Comp. Auth.	Comp. Auth.	✔	state	exercising	✘	**N33.3.1**	**S33.3.1**	✘
4.1	MS	MS	✔	ensure	ensure	✔	-	-	-
4.1.a	-	-	-	-	-	-	**N33.4.a**	**S33.4.a**	✔
4.1.b	-	-	-	-	-	-	**N33.4.b**	**S33.4.b**	✔
4.1.c	-	-	-	-	-	-	**N33.4.c**	**S33.4.c**	✔
4.1.d	-	-	-	-	-	-	**N33.4.d**	**S33.4.d**	✔
4.1.e	-	-	-	-	-	-	**N33.4.e**	**S33.4.e**	✔
4.1.f	-	-	-	-	-	-	**N33.4.f**	**S33.4.f**	✔
4.1.g	-	-	-	-	-	-	**N33.4.g**	**S33.4.g**	✔
4.1.h	-	-	-	-	-	-	**N33.4.h**	**S33.4.h**	✔
5.1	Article 32(6), (7) and (8)	Article 32(6), (7) and	❙	apply	NONE	✘	**N33.5.1**	**S33.5.1**	✘
6.1	MS	MS	✔	ensure	ensure	✔	**N33.6.1**	**S33.6.1**	✔
6.2	MS	MS	✔	ensure	ensure	✔	**N33.6.2**	**S33.6.2**	✔
	Sub-HIT % = 93.75 %			**Sub-HIT % = 75 %**			**Obj-HIT % = 90 %**		

Article 34

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1	MS	MS	✔	ensure	ensure	✔	**N34.1.1**	**S34.1.1**	✘
2	Administrative fines	-	✘	be imposed	-	✘	**N34.2.1**	**S34.2.1**	✔
3	Due regard	Due regard	✔	be given	deciding	✘	**N34.3.1**	**S34.3.1**	✘
4	MS	MS	✔	ensure	ensure	✔	**N34.4.1**	**S34.4.1**	✔
5	MS	MS	✔	ensure	ensure	✔	**N34.5.1**	**S34.5.1**	✔
6	MS	MS	✔	provide	impose	✘	**N34.6.1**	**S34.6.1**	✘
7	MS	MS	✔	lay	lay	✔	**N34.7.1**	**S34.7.1**	✔
8.1	MS	MS	✔	ensure	ensure	✔	**N34.8.1**	**S34.8.1**	✔
8.2	the fines imposed	the fines imposed	✔	be	be	✔	**N34.8.2**	**S34.8.2**	✔
8.2	MS	MS	✔	notify	notify	✔	**N34.8.3**	**S34.8.3**	❙
	Sub-HIT % = 90 %			**Sub-HIT % = 70 %**			**Obj-HIT % = 65 %**		

Article 35

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	-	-	-	-	-	-	-	-	-
2.1	-	-	-	-	-	-	-	-	-
2.2	Comp. Auth.	Comp. Auth.	✔	impose	impose	✔	**N35.2.2**	**S35.2.2**	❙
	Sub-HIT % = 100 %			**Sub-HIT % = 100 %**			**Obj-HIT % = 50 %**		

Article 36

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	-	-	-	-	-	-	-	-	-
2.1	-	-	-	-	-	-	-	-	-
2.2	Comp. Auth.	Comp. Auth.	✔	impose	impose	✔	**N35.2.2**	**S35.2.2**	❙
	Sub-HIT % = 100 %			**Sub-HIT % = 100%**			**Obj-HIT % = 50 %**		

Article 37

N.	Sub	I-Sub	Sub-HIT	Verb	I-Verb	Verb-HIT	Obj	I-Obj	Obj-HIT
1.1	-	-	-	-	-	-	-	-	-
1.2	That cooperation	That cooperation	✔	entail	entail	✔	-	-	-
1.2.a	-	-	-	-	-	-	??	??	✔
1.2.b	-	-	-	-	-	-	??	??	✔
1.2.c	-	-	-	-	-	-	??	??	✔
2	??	??	✔	??	??	✔	??	??	✔
	Sub-HIT % = 100 %			**Sub-HIT % = 100%**			**Obj-HIT % = 100 %**		

Article 7

Item 7.1

Hand

N7.1.1 A national cybersecurity strategy

- **N7.1.2.a** Objectives and priorities of the Member State's cybersecurity strategy covering in particular the sectors referred to in Annexes I and II
- **N7.1.2.b** A governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2
- **N7.1.2.c** a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts
- **N7.1.2.d** A mechanism to identify relevant assets and an assessment of the risks in that Member State
- **N7.1.2.e** an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors
- **N7.1.2.f** a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy
- **N7.1.2.g** A policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate
- **N7.1.2.h** A plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens

Spacy

S7.1.1 A national cybersecurity strategy

- **S7.1.2.a** Objectives and priorities of the Member State's cybersecurity strategy covering in particular the sectors
- **S7.1.2.b** A governance framework to achieve the objectives and priorities
- **S7.1.2.c** The roles and responsibilities of relevant stakeholders at national level
- **S7.1.2.d** A mechanism to identify relevant assets and an assessment of the risks in that Member State
- **S7.1.2.e** an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors
- **S7.1.2.f** a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy

S7.1.2.g a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate

S7.1.2.h A plan, including necessary measures

Item 7.2

Hand

N7.2.1

N7.2.1.a policies addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services

N7.2.1.b on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products

N7.2.1.c managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1)

N7.2.1.d policies related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables

N7.2.1.e promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures

N7.2.1.f promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities

N7.2.1.g supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure

N7.2.1.h including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law

N7.2.1.i strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs

N7.2.1.j promoting active cyber protection

Spacy

S7.2.1

S7.2.1.a policies addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services
S7.2.1.b policies on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement

S7.2.1.c policies managing vulnerabilities
S7.2.1.d policies related to sustaining the general availability, integrity and confidentiality of the public core of the open internet
S7.2.1.e promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures
S7.2.1.f policies promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives
S7.2.1.g supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure
S7.2.1.h including relevant procedures and appropriate information-sharing tools

S7.2.1.i policies strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises
S7.2.1.j promoting active cyber protection

Item 7.3

Hand

N7.3.1 their national cybersecurity strategies to the Commission within three months of their adoption
N7.3.2 information which relates to their national security from such notifications

Spacy

S7.3.1 Their national cybersecurity strategies
S7.3.2 information which relates to their national security from such notifications

Item 7.4

Hand

N7.4.1 their national cybersecurity strategies on a regular basis
N7.4.2 Member State in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strateg

Spacy

S7.4.1 Their national cybersecurity strategies
S7.4.2 a)Member States — b) upon their request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive

Article 8

Item 8.1

Hand

N8.1 Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities)

Spacy

S8.1 one or more competent authorities responsible for cybersecurity

Item 8.2

Hand

N8.2 the implementation of this Directive at national level

Spacy

S8.2 the implementation of this Directive at national level

Item 8.3

Hand

N8.3.1 a single point of contact
N8.3.2 that competent authority shall also be the single point of contact for that Member State

Spacy

S8.3.1 a single point of contact
S8.3.2 only one competent authority

Item 8.4

Hand

N8.4 a liaison function to ensure cross-border cooperation of its Member State's authorities

Spacy

S8.4 a liaison function

Item 8.5

Hand

N8.5 that their competent authorities and single points of contact have adequate resources to carry out, in an effective and efficient manner

Spacy

S8.5 a) that their competent authorities and single points of contact have adequate resources to carry out, in an effective and efficient manner — b)adequate resources

Item 8.6

Hand

N8.6.1 the Commission without undue delay of the identity of the competent authority referred to in paragraph 1 and of the single point of contact referred to in paragraph 3, of the tasks of those authorities, and of any subsequent changes thereto
N8.6.2 public the identity of its competent authority
N8.6.3 a list of the single points of contact publicly available

Spacy

S8.6.1 the commission
S8.6.2 public the identity of its competent authority
S8.6.3 a list of the single points of contact publicly available

Article 9

Item 9.1

Hand

N9.1.1 one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities)

N9.1.2 adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them

N9.1.3 coherence with the existing frameworks for general national crisis management

Spacy

S9.1.1 one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities)

S9.1.2 adequate resources

S9.1.3 coherence with the existing frameworks for general national crisis management

Item 9.2

Hand

N9.2 which of those authorities is to serve as the coordinator for the management of large-scale cybersecurity incidents and crises

Spacy

S9.2 which of those authorities is to serve as the coordinator for the management of large-scale cybersecurity incidents and crises

Item 9.3

Hand

N9.3 capabilities, assets and procedures that can be deployed in the case of a crisis for the purposes of this Directive

Spacy Item 9.3

S9.3 capabilities, assets and procedures that can be deployed in the case of a crisis for the purposes of this Directive

Item 9.4

Hand

N9.4.1 a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out

N9.4.2

N9.4.2.a the objectives of national preparedness measures and activities

N9.4.2.b the tasks and responsibilities of the cyber crisis management authorities

N9.4.2.c the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels

N9.4.2.d national preparedness measures, including exercises and training activities

N9.4.2.e the relevant public and private stakeholders and infrastructure involved

N9.4.2.f national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.

Spacy

S9.4.1 a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out

S9.4.2

S9.4.2.a NONE

S9.4.2.b NONE

S9.4.2.c NONE

S9.4.2.d NONE

S9.4.2.e NONE

S9.4.2.f NONE

Item 9.5

N9.5.1 the Commission of the identity of its authority

N9.5.2 to the Commission and to the European cyber crisis liaison organisation network (EU-CyCLONe) relevant information relating to the requirements of paragraph 4 about their national large-scale cybersecurity incident and crisis response plans within three months of the adoption of those plans.

N9.5.3 information where and to the extent that such exclusion is necessary for their national security

Spacy

S9.5.1 the Commission of the identity of its authority
S9.5.2 NONE
S9.5.3 information

Article 10

Item 10.1

Hand

N10.1.1 one or more CSIRTs
N10.1.2 within a competent authority.
N10.1.3 MULTIPLE OBJECTS

Spacy

S10.1.1 one or more CSIRTs
S10.1.2 NONE
S10.1.3 NONE

Item 10.2

Hand

N10.2 that each CSIRT has adequate resources to carry out effectively its tasks as set out in Article 11(3)

Spacy

S10.2 that each CSIRT has adequate resources to carry out effectively its tasks as set out in Article 11(3)

Item 10.3

Hand

N10.3.1 that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders
N10.3.2 that each CSIRT contributes to the deployment of secure information-sharing tools

Spacy

S10.3.1 that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders

S10.3.2 that each CSIRT contributes to the deployment of secure information-sharing tools

Item 10.4

Hand

N10.4 relevant information in accordance with Article 29

Spacy

S10.4 relevant information

Item 10.5

Hand

N10.5 in peer reviews organised in accordance with Article 19

Spacy

S10.5 NONE

Item 10.6

Hand

N10.6 the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network

Spacy

S10.6 the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network

Item 10.7

Hand

N10.7.1 cooperation relationships with third countries' national computer security incident response teams

N10.7.2 information exchange with those third countries' national computer security incident response teams

N10.7.3 relevant information with third countries' national computer security incident response teams

Spacy

S10.7.1 cooperation relationships with third countries' national computer security incident response teams

S10.7.2 information exchange with those third countries' national computer security incident response teams

S10.7.3 relevant information with third countries' national computer security incident response teams

Item 10.8

Hand

N10.8 with third countries' national computer security incident response teams

Spacy

S10.8 NONE

Item 10.9

Hand

N10.9 the commission of their respective tasks in relation to essential and important entities

Spacy

S10.9 the commission

Item 10.10

Hand

N10.10 the assistance of ENISA in developing their CSIRTs

Spacy

S10.10 the assistance of ENISA

Article 11

Item 11.1

Hand

N11.1.1

N11.1.2.a a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times; they shall clearly specify the communication channels and make them known to constituency and cooperative partners;

N11.1.2.b located at secure sites

N11.1.2.c with an appropriate system for managing and routing requests

N11.1.2.d the CSIRTs shall ensure the confidentiality and trustworthiness of their operations

N11.1.2.e availability of their services and their staff is trained appropriately

N11.1.2.f redundant systems and backup working space to ensure continuity of their service

Spacy

S11.1.1

S11.1.2.a a high level of availability of their communication channels

S11.1.2.b NONE

S11.1.2.c NONE

S11.1.2.d the CSIRTs shall ensure the confidentiality and trustworthiness of their operations

S11.1.2.e availability of their services

S11.1.2.f NONE

Item 11.2

Hand

N11.2.1 that their CSIRTs jointly have the technical capabilities necessary to carry out the tasks referred to in paragraph 3

N11.2.2 that sufficient resources are allocated to their CSIRTs to ensure adequate staffing levels for the purpose of enabling the CSIRTs to develop their technical capabilities

Spacy

S11.2.1 that their CSIRTs jointly have the technical capabilities necessary to carry out the tasks referred to in paragraph 3

S11.2.2 that sufficient resources are allocated to their CSIRTs to ensure adequate staffing levels for the purpose of enabling the CSIRTs to develop their technical capabilities

11.3

—

Item 11.4

Hand

N11.4.1 cooperation relationships with relevant stakeholders in the private sector

Spacy

S11.4.1 cooperation relationships with relevant stakeholders in the private sector

Item 11.5

Hand

N11.5.1.a the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to incident-handling procedures
N11.5.1.b (b) crisis management
N11.5.1.c coordinated vulnerability disclosure under Article 12(1).

Spacy

S11.5.1.a NONE
S11.5.1.b NONE
S11.5.1.c NONE

Article 12

Item 12.1

Hand

N12.1.1 one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure
N12.1.2 a trusted intermediary
N12.1.3
- **N12.1.3.a** identifying and contacting the entities concerned
- **N12.1.3.b** assisting the natural or legal persons reporting a vulnerability
- **N12.1.3.c** negotiating disclosure timelines and managing vulnerabilities that affect multiple entities

Spacy

S12.1.1 one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure
S12.1.2 the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party
S12.1.3
S12.1.3.a identifying and contacting the entities concerned
S12.1.3.b assisting the natural or legal persons reporting a vulnerability
S12.1.3.c negotiating disclosure timelines and managing vulnerabilities that affect multiple entities

Item 12.2

Hand

N12.2.1 a vulnerability database
N12.2.2 TO-DO
N12.2.3 TO-DO

Spacy

S12.2.1 the Cooperation Group, a European vulnerability database
S12.2.2 TO-DO
S12.2.3 TO-DO

Article 13

Item 13.1

Hand

N13.1.1 with each other with regard to the fulfilment of the obligations laid down in this Directive

Spacy

S13.1.1 NONE

Item 13.2

Hand

N13.2.1 their competent authorities, receive notifications of significant incidents pursuant to Article 23, and incidents, cyber threats and near misses pursuant to Article 30

Spacy

S13.2.1 their competent authorities, receive notifications of significant incidents pursuant to Article 23, and incidents, cyber threats and near misses pursuant to Article 30

Item 13.3

Hand

N13.3.1 their competent authorities inform their single points of contact of notifications of incidents, cyber threats and near misses submitted pursuant to this Directive

Spacy

S13.3.1 their competent authorities inform their single points of contact of notifications of incidents, cyber threats and near misses submitted pursuant to this Directive

Item 13.4

Hand

N13.4.1 appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, the national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, the competent authorities under Regulation (EU) 2022/2554, the national regulatory authorities under Directive (EU) 2018/1972, the competent authorities under Directive (EU) 2022/2557, as well as the competent authorities under other sector-specific Union legal acts, within that Member State

Spacy

S13.4.1 appropriate cooperation between those bodies and law enforcement authorities, data protection authorities

Item 13.5

Hand

N13.5.1 that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to such risks, threats and incidents

N13.5.2 t their competent authorities under this Directive and their competent authorities under Regulation (EU) No 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats

Spacy

S13.5.1 that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to such risks, threats and incidents

S13.5.2 relevant information

Hand

N13.6.1 through technical means for notifications referred to in Articles 23 and 30

Spacy

S13.6.1 the report through technical

Article 14

Item 14.1

Hand

N14.1.1 PASSIVE - NONE

Spacy

S14.1.1 PASSIVE - NONE

Item 14.2

Hand

N14.2.1 its tasks on the basis of biennial work programmes referred to in paragraph 7

Spacy

S14.2.1 its tasks on the basis of biennial work programmes referred to in paragraph 7

Item 14.2

Hand

N14.2.1 its tasks on the basis of biennial work programmes referred to in paragraph 7

Spacy

S14.2.1 its tasks on the basis of biennial work programmes referred to in paragraph 7

Item 14.3

Hand

N14.3.1 of representatives of Member States, the Commission and ENISA
N14.3.2 in the activities of the Cooperation Group as an observer
N14.3.3 in the activities of the Cooperation Group in accordance with Article 47(1) of that Regulation.

Spacy

S14.3.1 NONE
S14.3.2 NONE
S14.3.3 NONE

Item 14.4

Hand

S14.4.1
S14.1.1.a TO-DO

Spacy

Item 14.5

Hand

N14.5.1 cooperation of their representatives in the Cooperation Group

Spacy

S14.5.1 cooperation of their representatives in the Cooperation Group

Item 14.6

Hand

N14.6.1 a technical report on selected topics

Spacy

S14.6.1 a technical report on selected topics

Item 14.7

Hand

N14.7.1 a work programme in respect of actions to be undertaken to implement its objectives and tasks

Spacy

S14.7.1 a work programme in respect of actions to be undertaken to implement its objectives and tasks

Item 14.8

Hand

N14.8.1 acts laying down procedural arrangements necessary for the functioning of the Cooperation Group

Spacy

S14.8.1 acts laying down procedural arrangements necessary for the functioning of the Cooperation Group

Item 14.9

Hand

N14.9.1 on a regular basis and in any event at least once a year with the Critical Entities Resilience Group established under Directive (EU) 2022/2557 to promote and facilitate strategic cooperation and the exchange of information Group

Spacy

S14.9.1 strategic cooperation and the exchange of information

Article 15

Item 15.1

Hand

N15.1.1 PASSIVE

Spacy

S15.1.1 PASSIVE

Item 15.2

Hand

N15.2.1 PASSIVE
N15.2.2 in the CSIRTs network as an observer
N15.2.3 the secreteriat - assistance for the cooperation among the CSIRTs.

Spacy

S15.2.1 PASSIVE
S15.2.2 NONE
S15.2.3 the secretariat

Item 15.3

Hand

N15.3.1

N15.3.1.a to exchange information about the CSIRTs' capabilities
N15.3.1.b to facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs
N15.3.1.c to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities
N15.3.1.d to exchange information with regard to cybersecurity publications and recommendations
N15.3.1.e to ensure interoperability with regard to information-sharing specifications and protocols
N15.3.1.f at the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities
N15.3.1.g at the request of a member of the CSIRTs network, to discuss and, where possible, implement a coordinated response to an incident that has been identified within the jurisdiction of that Member State

N15.3.1.h to provide Member States with assistance in addressing cross-border incidents pursuant to this Directive

N15.3.1.i to cooperate, exchange best practices and provide assistance to the CSIRTs designated as coordinators pursuant to Article 12(1) with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one Member State

N15.3.1.j to discuss and identify further forms of operational cooperation, including in relation to:(i) categories of cyber threats and incidents;(ii) early warnings;(iii) mutual assistance;(iv) principles and arrangements for coordination in response to cross-border risks and incidents;(v) contribution to the national large-scale cybersecurity incident and crisis response plan referred to in Article 9(4) at the request of a Member State

N15.3.1.k to inform the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (j), and, where necessary, request guidance in that regard

N15.3.1.l to take stock of cybersecurity exercises, including those organised by ENISA

N15.3.1.m at the request of an individual CSIRT, to discuss the capabilities and preparedness of that CSIRT

N15.3.1.n to cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and cyber threats across the Union

N15.3.1.o where relevant, to discuss the peer-review reports referred to in Article 19(9)

N15.3.1.p to provide guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation

Spacy

S15.3.1

S15.3.1.a idem

S15.3.1.b idem

S15.3.1.c idem

S15.3.1.d idem

S15.3.1.e idem

S15.3.1.f idem

S15.3.1.g idem

S15.3.1.h idem

S15.3.1.i idem

S15.3.1.j idem

S15.3.1.k idem

S15.3.1.l idem

S15.3.1.m idem

S15.3.1.n idem

S15.3.1.o idem

S15.3.1.p idem

Item 15.4

Hand

N15.4.1 the progress made with regard to the operational cooperation and adopt a report
N15.4.2 conclusions and recommendations on the basis of the outcome of the peer reviews
N15.4.3 to the cooperation group

Spacy

S15.4.1 the progress made with regard to the operational cooperation and adopt a report
S15.4.2 conclusions and recommendations on the basis of the outcome of the peer reviews
S15.4.3 NONE

Item 15.5

Hand

N15.5.1 its rules of procedure

Spacy

S15.5.1 its rules of procedure

Item 15.6

Hand

N15.6.1 on procedural arrangements and cooperate on the basis thereof

Spacy

S15.6.1 NONE

Article 16

Item 16.1

Hand

N16.1.1 the coordinated management of large-scale cybersecurity incidents and crises

Spacy

S16.1.1 the coordinated management of large-scale cybersecurity incidents and crises

Item 16.2

Hand

N16.2.1 of the representatives of Member States' cyber crisis management authorities

N16.2.2 in the activities of EU-CyCLONe as an observer

Spacy

S16.2.1 NONE
S16.2.2 NONE

Item 16.3

Hand

N16.3.1
- **N16.3.1.a** to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises
- **N16.3.1.b** to develop a shared situational awareness for large-scale cybersecurity incidents and crises
- **N16.3.1.c** to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures
- **N16.3.1.d** to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises
- **N16.3.1.e** to discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4)

Spacy

S16.3.1
- **S16.3.1.a** idem
- **S16.3.1.b** idem
- **S16.3.1.c** idem
- **S16.3.1.d** idem
- **S16.3.1.e** idem

Item 16.4

Hand

N16.4.1 its rules of procedure

Spacy

S16.4.1 its rules of procedure

Item 16.5

Hand

N16.5.1 on a regular basis to the Cooperation Group on the management of large-scale cybersecurity incidents and crises, as well as trends, focusing in particular on their impact on essential and important entities

Spacy

S16.5.1 important entities

Item 16.6

Hand

N16.6.1 with the CSIRTs network on the basis of agreed procedural arrangements provided for in Article 15(6)

Spacy

S16.6.1 NONE

Item 16.7

Hand

N16.7.1 a report assessing its work

Spacy

S16.7.1 a report assessing its work

Article 17

Item 17.1

Hand

N17.1.1 —-

Spacy

S17.1.1 —-

Article 18

Item 18.1

Hand

N18.1.1 TO-DO
N18.1.2

N18.1.2.a a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape

N18.1.2.b an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union

N18.1.2.c an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises

N18.1.2.d an aggregated assessment of the outcome of the peer reviews referred to in Article 19

N18.1.2.e an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level, as well as of the extent to which the Member States' national cybersecurity strategies are aligned

Spacy

S18.1.1 TO-DO
S18.1.2

S18.1.2.a idem
S18.1.2.b idem
S18.1.2.c idem
S18.1.2.d idem
S18.1.2.e idem

Item 18.2

Hand

N18.2.1 particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of regulation (EU) 2019/881

Spacy

S18.2.1 particular policy recommendations with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7

Item 18.3

Hand

N18.3.1 the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e)

Spacy

S18.3.1 the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e)

Article 19

Item 19.1

Hand

N19.1.1 the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive

N19.1.2 by cybersecurity experts
N19.1.3 by at least two Member States, different from the Member State being reviewed

Spacy

S19.1.1 mutual trust
S19.1.2 NONE
S19.1.3 NONE

Item 19.2

Hand

N19.2.1 objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States designate cybersecurity experts eligible to carry out the peer reviews
N19.2.2 as observers in the peer reviews

Spacy

S19.2.1 objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States designate cybersecurity experts eligible to carry out the peer reviews
S19.2.2 NONE

Item 19.3

Hand

N19.3.1 specific issues as referred to in paragraph 1, point (f), for the purposes of a peer review

Spacy

S19.3.1 specific issues

Item 19.4

Hand

N19.4.1 the participating Member States of its scope, including the specific issues identified pursuant to paragraph 3

Spacy

S19.4.1 the participating Member States of its scope

Item 19.5

Hand

N19.5.1 a self-assessment of the reviewed aspects — that self-assessment to the designated cybersecurity expert
N19.5.2 the methodology for the Member States' self-assessment

Spacy

S19.5.1 a self-assessment of the reviewed aspects
S19.5.2 the methodology for the Member States' self-assessment

Item 19.6

Hand

N19.6.1 physical or virtual on-site visits and off-site exchanges of information
N19.6.2 the designated cybersecurity experts with the information necessary for the assessment
N19.6.3 appropriate codes of conduct underpinning the working methods of designated cybersecurity experts
N19.6.4 for that purpose
N19.6.5 any sensitive or confidential information obtained in the course of that peer review to any third parties

Spacy

S19.6.1 physical or virtual on-site visits and off-site exchanges of information
S19.6.2 the designated cybersecurity experts with the information necessary for the assessment
S19.6.3 appropriate codes of conduct underpinning the working methods of designated cybersecurity experts
S19.6.4 NONE
S19.6.5 any sensitive or confidential information obtained in the course of that peer review to any third parties

Item 19.7

Hand

N19.7.1 subject to a further peer review in that Member State for two years following the conclusion of the peer review, unless otherwise requested by the Member State or agreed upon after a proposal of the Cooperation Group.

Spacy

S19.7.1 NONE

Item 19.8

Hand

N19.8.1 that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review
N19.8.2 to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State

Spacy

S19.8.1 that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review
S19.8.2 to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State

Item 19.9

Hand

N19.9.1 reports on the findings and conclusions of the peer reviews
N19.9.2 comments on the draft reports
N19.9.3 recommendations to enable improvement on the aspects covered by the peer review
N19.9.4 to the Cooperation Group and the CSIRTs network
N19.9.5 to make its report, or a redacted version of it, publicly available

Spacy

S19.9.1 reports on the findings and conclusions of the peer reviews
S19.9.2 comments on the draft reports
S19.9.3 recommendations to enable improvement on the aspects covered by the peer review
S19.9.4 NONE
S19.9.5 to make its report, or a redacted version of it

Article 20

.1 Item 20.1

Hand

N20.1.1 the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article

Spacy

S20.1.1 the cybersecurity risk-management measures taken by those entities in order to comply with Article 21

Item 20.2

Hand

N20.2.1 that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity

Spacy

S20.2.1 that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity

Article 21

TO - DO

Item 21.1

Hand

N21.1.1 essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Spacy

S21.1.1 appropriate and proportionate technical, operational and organisational measures

Article 22

Item 22.1

Hand

N22.1.1 coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors

Spacy

S22.1.1 coordinated security risk assessments of specific critical ICT services

Item 22.2

Hand

N22.2.1 the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1

Spacy

S22.2.1 the specific critical ICT services

Article 23

Item 23.1

Hand

N23.1.1 that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3

N23.1.2 the recipients of their services of significant incidents that are likely to adversely affect the provision of those services

N23.1.3 that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident

N23.1.4 the notifying entity to increased liability

Spacy

S23.1.1 that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3

S23.1.2 the recipients of their services of significant incidents that are likely to adversely affect the provision of those services

S23.1.3 that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident

S23.1.4 the notifying entity to increased liability

Item 23.2

Hand

N23.2.1 that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat

N23.2.2 those recipients of the significant cyber threat itself

Spacy

S23.2.1 that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat

S23.2.2 those recipients of the significant cyber threat itself

Item 23.3

Hand

N23.3.1

N23.3.1.a to be significant if it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned

N23.3.1.b to be significant if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage

Spacy

S23.3.1

S23.3.1.a to be significant if it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned

S23.3.1.b to be significant if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage

Item 23.4

Hand

N23.4.1

N23.4.1.a TO-DO

Spacy

S23.3.1

S23.3.1.a TO- DO

Item 23.5

Hand

N23.5.1 a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures
N23.5.2 NOT REPRESENTABLE
N23.5.3 additional technical support
N23.5.4 guidance on reporting the significant incident to law enforcement authorities

Spacy

S23.5.1 a response to the notifying entity, including initial feedback on the significant incident and
S23.5.2 NOT REPRESENTABLE
S23.5.3 additional technical support
S23.5.4 guidance on reporting the significant incident to law enforcement authorities

Item 23.6

Hand

N23.6.1 the other affected Member States and ENISA of the significant incident
N23.6.2 the type of information received in accordance with paragraph 4
N23.6.3 the entity's security and commercial interests as well as the confidentiality of the information provided

Spacy

S23.6.1 the other affected Member States and ENISA of the significant incident
S23.6.2 the type of information received in accordance with paragraph 4
S23.6.3 the entity's security and commercial interests

Item 23.7

Hand

N23.7.1 the public about the significant incident or require the entity to do so

Spacy

S23.7.1 a significant incident

Item 23.8

Hand

N23.8.1 notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.

Spacy

S23.8.1 NONE

Item 23.9

Hand

N23.9.1 a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 3

N23.9.2 technical guidance on the parameters of the information to be included in the summary report

N23.9.3 the Cooperation Group and the CSIRTs network about its findings on notifications received every six months

Spacy

S23.9.1 a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 3

S23.9.2 technical guidance on the parameters of the information to be included in the summary report

S23.9.3 the Cooperation Group and the CSIRTs network about its findings on notifications received every six months

Item 23.10

Hand

N23.10.1 to the competent authorities under Directive (EU) 2022/2557 information about significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30 by entities identified as critical entities under Directive (EU) 2022/2557

Spacy

S23.10.1 NONE

Item 23.11

Hand

N23.11.1 implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 of this Article and to Article 30 and of a communication submitted pursuant to paragraph 2 of this Article

Spacy

S23.11.1 NONE

Article 24

Item 24.1

Hand

N24.1.1 essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881

N24.1.2 essential and important entities to use qualified trust services

Spacy

S24.1.1 ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881, essential and important entities to use particular ICT products

S24.1.2 essential and important entities, to use qualified trust services

Item 24.2

Hand

N24.2.1 adopt delegated acts, in accordance with Article 38, to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881

N24.2.2 where insufficient levels of cybersecurity have been identified and shall include an implementation period

Spacy

S24.2.1 to adopt delegated acts
S24.2.2 an implementation period

Item 24.3

Hand

N24.3.1 ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881

Spacy

S24.3.1 the Cooperation Group and the European Cybersecurity Certification Group

Article 25

Item 25.1

Hand

N25.1.1 the use of European and international standards and technical specifications relevant to the security of network and information systems

Spacy

S25.1.1 the convergent implementation of Article 21

Item 25.2

Hand

N25.2.1 advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered

Spacy

S25.2.1 relevant stakeholders

Article 26

Item 26.1

Hand

N26.1.1 TO-DO

Spacy

S26.1.1 TO-DO

Item 26.2

Hand

N26.2.1 — — —
N26.2.2 — — —

Spacy

S26.2.1 — — —
S26.2.2 — — —

Article 27

Item 27.1

Hand

N27.1.1 a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact in accordance with paragraph 4
N27.1.2 the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable

Spacy

S27.1.1 TLD name registries
S27.1.2 the competent authorities access to that registry

Item 27.2

Hand

N27.2.1
N27.2.1.a entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 the name of the entity

N27.2.1.b entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable

N27.2.1.c entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3)

N27.2.1.d entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3)

N27.2.1.e entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 the Member States where the entity provides services

N27.2.1.f entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025

Spacy

S27.2.1

S27.2.1.a entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 the name of the entity

S27.2.1.b entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable

S27.2.1.c entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3)

S27.2.1.d entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 up-to-date contact details, including email addresses and telephone numbers of the entity

S27.2.1.e entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025 the Member States where the entity provides services

S27.2.1.f entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025

Item 27.3

Hand

N27.3.1 that the entities referred to in paragraph 1 notify the competent authority about any changes to the information they submitted under paragraph 2 without delay and in any event within three months of the date of the change

Spacy

S27.1.1 that the entities referred to in paragraph 1 notify the competent authority about any changes to the information they submitted under paragraph 2 without delay and in any event within three months of the date of the change

Article 28

Item 28.1

Hand

N28.1.1 TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data

Spacy

S28.1.1 TLD name registries and entities , providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data

Item 28.2

Hand

N28.2.1 the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLD

N28.2.2

N28.2.2.a the domain name

N28.2.2.b the date of registration

N28.2.2.c the registrant's name, contact email address and telephone number

N28.2.2.d the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant

Spacy

S28.2.1 TLD name registries
S28.2.2
S28.2.2.a the domain name
S28.2.2.b the date of registration
S28.2.2.c the registrant's name, contact email address and telephone number
S28.2.2.d the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant

Item 28.3

Hand

N28.3.1 the TLD name registries and the entities providing domain name registration services to have policies and procedures
N28.3.2 such policies and procedures to be made publicly available

Spacy

S28.3.1 the TLD name registries and the entities providing domain name registration services to have policies and procedures
S28.3.2 such policies and procedures to be made publicly available

Item 28.4

Hand

N28.4.1 the TLD name registries and the entities providing domain name registration services

Spacy

S28.4.1 the TLD name registries and the entities providing domain name registration services

Item 28.5

Hand

N28.5.1 the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers
N28.5.2 the TLD name registries and the entities providing domain name registration services
N28.5.3 policies and procedures with regard to the disclosure of such data to be made publicly available

Spacy

S28.5.1 the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers
S28.5.2 the TLD name registries and the entities providing domain name registration services
S28.5.3 policies and procedures

Item 28.6

Hand

N28.6.1 in a duplication of collecting domain name registration data
N28.6.2 TLD name registries and entities , providing domain name registration services to cooperate with each other

Spacy

S28.6.1 domain name registration data
S28.6.2 TLD name registries and entities, providing domain name registration services to cooperate with each other

Article 29

Item 29.1

Hand

N29.1.a guardare testo
N29.1.b

Spacy

S29.1.a that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive
S29.1.b that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive

Item 29.2

Hand

N29.2.1 that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers
N29.2.2 through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared

Spacy

S29.2.1 that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers

S29.2.2 NONE

Item 29.3

Hand

N29.3.1 the establishment of cybersecurity information-sharing arrangements

N29.3.2 operational elements including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements

N29.3.3 conditions on the information made available by the competent authorities or the CSIRTs.

Spacy

S29.3.1 the establishment of cybersecurity information-sharing arrangements

S29.3.2 operational elements including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements

S29.3.3 conditions on the information made available by the competent authorities or the CSIRT

Item 29.4

Hand

N29.4.1 that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements

Spacy

S29.4.1 that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements

Item 29.5

Hand

N29.5.1 assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance

Spacy

S29.5.1 assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance

Article 30

Item 30.1

Hand

N30.1.a that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by essential and important entities with regard to incidents, cyber threats and near misses

N30.1.b that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses

Spacy

S30.1.a that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by essential and important entities with regard to incidents, cyber threats and near misses

S30.1.b that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses

Item 30.2

Hand

N30.2.1 the notifications referred to in paragraph 1 of this Article in accordance with the procedure laid down in Article 23

N30.2.2 the processing of mandatory notifications over voluntary notifications

Spacy

S30.2.1 the notifications referred to in paragraph 1 of this Article in accordance with the procedure laid down in Article 23

S30.2.2 the processing of mandatory notifications over voluntary notifications

Article 31

Item 31.1

Hand

N31.1.1 that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive

Spacy

S31.1.1 that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive

Item 31.2

Hand

N31.2.1 their competent authorities, to prioritise supervisory tasks
N31.2.2 NONE
N31.2.3 supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach

Spacy

S31.2.1 their competent authorities, to prioritise supervisory tasks
S31.2.2 NONE
S31.2.3 their supervisory tasks provided for in Articles 32 and 33

Item 31.3

Hand

N31.3.1 in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation.

Spacy

S31.3.1 NONE

Item 31.4

Hand

N31.4.1 that, in the supervision of compliance of public administration entities with this Directive and the imposition of enforcement measures with regard to infringements of this Directive, the competent authorities have appropriate powers to carry out such tasks with operational independence vis-à-vis the public administration entities supervised

N31.4.2 on the imposition of appropriate, proportionate and effective supervisory and enforcement measures in relation to those entities in accordance with the national legislative and institutional frameworks.

Spacy

S31.4.1 that, in the supervision of compliance of public administration entities with this Directive and the imposition of enforcement measures with regard to infringements of this Directive, the competent authorities have appropriate powers to carry out such tasks with operational independence vis-à-vis the public administration entities supervised

S31.4.2 NONE

Article 32

Item 32.1

Hand

N32.1.1 that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case

Spacy

S32.1.1 that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case

Item 32.2

Hand

N32.2.a that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to on-site inspections and off-site supervision, including random checks conducted by trained professionals

N32.2.b that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to regular and targeted security audits carried out by an independent body or a competent authority

N32.2.c that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity

N32.2.d that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned

N32.2.e that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27

N32.2.f that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to requests to access data, documents and information necessary to carry out their supervisory tasks

N32.2.g that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence

Spacy

S32.2.a that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to on-site inspections and off-site supervision, including random checks conducted by trained professionals

S32.2.b that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to regular and targeted security audits carried out by an independent body or a competent authority

S32.2.c that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity

S32.2.d that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to security scans based on objective, non-discriminatory, fair and transparent

risk assessment criteria, where necessary with the cooperation of the entity concerned

S32.2.e that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27

S32.2.f that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to requests to access data, documents and information necessary to carry out their supervisory tasks

S32.2.g that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence

Item 32.3

Hand

N32.3.1 the purpose of the request and specify the information requested.

Spacy

S32.3.1 NONE

Item 32.4

Hand

N32.4.1.a that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to issue warnings about infringements of this Directive by the entities concerned

N32.4.1.b that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive

N32.4.1.c that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct

N32.4.1.d that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period

N32.4.1.e that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat

N32.4.1.f that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline

N32.4.1.g that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23

N32.4.1.h that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to make public aspects of infringements of this Directive in a specified manner

N32.4.1.i that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph

Spacy

S32.4.1.a that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to issue warnings about infringements of this Directive by the entities concerned

S32.4.1.b that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive

S32.4.1.c that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct

S32.4.1.d that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period

S32.4.1.e that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat

S32.4.1.f that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline

S32.4.1.g that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23

S32.4.1.h that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to order the entities concerned to make public aspects of infringements of this Directive in a specified manner

S32.4.1.i that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph

Item 32.5

Hand

N32.5.1 that their competent authorities have the power to establish a deadline by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of those authorities.

N32.5.2

N32.5.2.a that their competent authorities have the power to suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity

N32.5.2.b that their competent authorities have the power to request that the relevant bodies, courts or tribunals, in accordance with national law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative

level in the essential entity from exercising managerial functions in that entity.

Spacy

S32.5.1 NONE

S32.5.2

S32.5.2.a that their competent authorities have the power to suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity

S32.5.2.b that their competent authorities have the power to request that the relevant bodies, courts or tribunals, in accordance with national law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity.

Item 32.6

Hand

N32.6.1 that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive.

N32.6.2 that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive

Spacy

S32.6.1 that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it

S32.6.2 that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive

Item 32.7

Hand

N32.7.1 the seriousness of the infringement and the importance of the provisions breached, the following, inter alia, constituting serious infringement in any event:(i) repeated violations;(ii) a failure to notify or remedy significant incidents;(iii) a failure to remedy deficiencies following binding instructions from competent authorities;(iv) the obstruction of audits or monitoring activities

ordered by the competent authority following the finding of an infringement; (v) providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations laid down in Articles 21 and 23

N32.7.2 the duration of the infringement

N32.7.3 any relevant previous infringements by the entity concerned

N32.7.4 any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected

N32.7.5 any intent or negligence on the part of the perpetrator of the infringement

N32.7.6 any measures taken by the entity to prevent or mitigate the material or non-material damage

N32.7.7 any adherence to approved codes of conduct or approved certification mechanisms

N32.7.8 the level of cooperation of the natural or legal persons held responsible with the competent authorities

Spacy

S32.7.1 NONE
S32.7.2 NONE
S32.7.3 NONE
S32.7.4 NONE
S32.7.5 NONE
S32.7.6 NONE
S32.7.7 NONE
S32.7.8 NONE

Item 32.8

Hand

N32.8.1 a detailed reasoning for their enforcement measures

N32.8.2 the entities concerned of their preliminary findings

N32.8.3 a reasonable time for those entities to submit observations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded

Spacy

S32.8.1 a detailed reasoning for their enforcement measures
S32.8.2 the entities concerned of their preliminary findings
S32.8.3 a reasonable time

Item 32.9

Hand

N32.9.1 that their competent authorities under this Directive inform the relevant competent authorities within the same Member State under Directive (EU) 2022/2557 when exercising their supervisory and enforcement powers aiming to ensure compliance of an entity identified as a critical entity under Directive (EU) 2022/2557 with this Directive

N32.9.2 the competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557

Spacy

S32.9.1 that their competent authorities under this Directive inform the relevant competent authorities within the same Member State under Directive (EU) 2022/2557 when exercising their supervisory and enforcement powers aiming to ensure compliance of an entity identified as a critical entity under Directive (EU) 2022/2557 with this Directive

S32.9.2 NONE

Item 32.10

Hand

N32.10.1 their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554

N32.10.2 that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554 with this Directive

Spacy

S32.10.1 that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554

S32.10.2 that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554 with this Directive

Article 33

Item 33.1

Hand

N33.1.1 that the competent authorities take action, where necessary, through ex-post supervisory measures

N33.1.2 that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case

Spacy

S33.1.1 that the competent authorities take action, where necessary, through ex post supervisory measures

S33.1.2 that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case

Item 33.2

Hand

N33.2.a that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to on-site inspections and off-site ex post supervision conducted by trained professionals

N33.2.b that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to targeted security audits carried out by an independent body or a competent authority

N33.2.c that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned

N33.2.d that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27

N33.2.e that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to requests to access data, documents and information necessary to carry out their supervisory tasks

N33.2.f that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence

Spacy

S33.2.a that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to on-site inspections and off-site ex post supervision conducted by trained professionals

S33.2.b that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to targeted security audits carried out by an independent body or a competent authority

S33.2.c that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned

S33.2.d that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27

S33.2.e that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to requests to access data, documents and information necessary to carry out their supervisory tasks

S33.2.f that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence

Item 33.3

Hand

N33.3.1 the purpose of the request and specify the information requested

Spacy

S33.3.1 NONE

Item 33.4

Hand

N33.4.a that the competent authorities, when exercising their enforcement powers in relation to important entities, have the power at least to issue warnings about infringements of this Directive by the entities concerned

N33.4.b adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of this Directive;

N33.4.c order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct

N33.4.d order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period

N33.4.e order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat

N33.4.f order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline

N33.4.g order the entities concerned to make public aspects of infringements of this Directive in a specified manner

N33.4.h impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (g) of this paragraph

Spacy

S33.4.a that the competent authorities, when exercising their enforcement powers in relation to important entities, have the power at least to issue warnings about infringements of this Directive by the entities concerned

S33.4.b adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of this Directive

S33.4.c order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct

S33.4.d order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period

S33.4.e order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat

S33.4.f order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline

S33.4.g order the entities concerned to make public aspects of infringements of this Directive in a specified manner

S33.4.h impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (g) of this paragraph

Item 33.5

Hand

N33.5.1 mutatis mutandis to the supervisory and enforcement measures provided for in this Article for important entities

Spacy

S33.5.1 NONE

Item 33.6

Hand

N33.6.1 that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554

N33.6.2 that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an important entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554 with this Directive

Spacy

S33.6.1 that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554

S33.6.2 that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an important entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554 with this Directive

A Article 34

Item 34.1

Hand

N34.1.1 that the administrative fines imposed on essential and important entities pursuant to this Article in respect of infringements of this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

Spacy

S34.1.1 that the administrative fines imposed on essential and important entities pursuant to this Article in respect of infringements of this Directive

Item 34.2

Hand

N34.2.1 n addition to any of the measures referred to in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g)

Spacy

S34.2.1 NONE

Item 34.3

Hand

N34.3.1 as a minimum, to the elements provided for in Article 32(7).

Spacy

S34.3.1 NONE

Item 34.4

Hand

N34.4.1 that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher

Spacy

S34.4.1 that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher

Item 34.5

Hand

N34.5.1 that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher

Spacy

S34.5.1 that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher

Item 34.6

Hand

N34.6.1 for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement of this Directive in accordance with a prior decision of the competent authority.

Spacy

S34.6.1 NONE

Item 34.7

Hand

N34.7.1 the rules on whether and to what extent administrative fines may be imposed on public administration entities.

Spacy

S34.7.1 the rules on whether and to what extent administrative fines may be imposed on public administration entities

Item 34.8

Hand

N34.8.1 that this Article is applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts or tribunals, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by the competent authorities.

N34.8.2 be effective, proportionate and dissuasive

N34.8.3 the provisions of the laws which it adopts pursuant to this paragraph by 17 October 2024

Spacy

S34.8.1 the rules on whether and to what extent administrative fines may be imposed on public administration entities
S34.8.2 be effective, proportionate and dissuasive
S34.8.3 the provisions of the laws which it adopts pursuant to this paragraph by 17 October 2024

Article 35

Item 35.1

Hand

N35.1.1 NONE
N35.1.2 NONE
N35.1.3 the enforcement measures provided for in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g), of this Directive

Spacy

S35.1.1 NONE
S35.1.2 NONE
S35.1.3 the enforcement measures provided for in Article 32(4)

Item 35.2

Hand

N35.2.1 NONE
N35.2.2 the enforcement measures provided for in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g), of this Directive

Spacy

S35.2.1 NONE
S35.2.2 the enforcement measures provided for in Article 32(4)