全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

“

”

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
全国网络安全标准化技术委员会
TC260
Cybersecurity

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

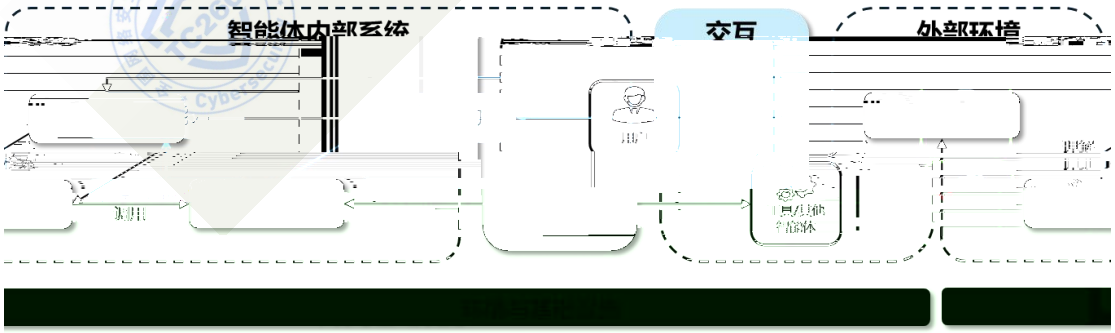
1 1
1.1 1
1.2 3
1.3 6
1.4 6
2 10
2.1 10
2.2 18
3 30
3.1 30
3.2 32
3.3 37
3.4 42
3.5 48
3.6 53
4 55
4.1 55
4.2 57
4.3 60

5 64
5.1 64
5.2 67
5.3 68
6 70
A 73
B 77
B.1 77
B.2 77
B.3 78
B.4 79
C 81
..... 84

1.1

1

ISO/IEC 22989:2022	
ITU-T F.748.46	
TC28	1



1

Agen ic AI	/	Agen Agen ic Welc ming Di e e A ache Kee Machine Lea ning S ng 2024	
Emb died AI		Emb died AI Ga ne ′ 2024 AI H e C cle_ Ke AI T e and T end	
la ge- ca le m del/la ge- cale dee lea n ing m del	/	1 GB/T 45288.1-2025	
machine lea ning			

model		GB/T 41867.1-2022 3.2.11	
artificial intelligence system		GB/T 41867.1-2022 3.2.8	

1.2 2 صم

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

(3)

(4)

(5)

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
全国网络安全标准化技术委员会 TC260 Cybersecurity

1.3

1

2

3

1.4

1.4.1

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

2024　　2025

(1)

(2)

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
TC260 Cybersecurity

(3)

(4)

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

1.4.2

(1)

Re ea ch and Ma ke [1] 2024

51 2030 471 2024 2030

44.8%

IBM

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

Sf Bank

(2)

2025 HAI

S anf! d In i e f! H man-Cen e ed AI

AI Inde Re! 2025 [2]

AI 2024

AI 2024

2523

1,508 44.5% AI

2024 1,091

93 12 45 24

AI 2024 290.4 +

254 AI

339 18.7%

2.1

2.1.1 AI

AI AI

AI

+ +

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

AI

2023 10

AI [3]

AI 1000

AI

AI

AI

2024 8 1 [4] EU AI Ac

+

AI

4

AI

7% 3500

1500 3%

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

AI

[5] AI

2022 AIDA [6]

2025

AI

AI

AI

1000 2023

[7] +

8

+

2024

[8] +

AI

AI

50

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

+ AI

2024 12 AI [9] AI

AI AI

AI

AI

2.1.2 AI

AI +

+ + +

2017 [10]

AI

AI AI

AI

AI

[11]

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

[12]

[13] AI

AI

2.0

6

AI

6

2025 10 28

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

2026 1 1

AI

2021

[14]

AI

2023 1 10

[15]

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

[16]

AI

AI

AI

AI

2023 7

[17] 2023 8 15

AI

AI +

AI

2025

4 AI

AI 3500

96 3700

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

+ +

2025 1 1 /

[18]

3

AI

2025 8 +

[19] +

2025 9

2.0 [20]

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

2

2.2.1

(1) ISO

ISO

ISO/IEC/JTC1/SC27

1 ISO/IEC TR 27563:2023 AI

1

ISO/IEC 27090

2 ISO/IEC 27091 S

– – ISO/IEC PWI 25240

[21] SC27 2025 9

ISO/IEC/JTC1/SC42 ó m"

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

Agen

ISO/IEC 23053:2022

ML

ISO/IEC 24029-1:2021 1

(2) ITU-T

ITU-T

ITU-T Y.3172

ITU-T Y.3500 Y.3500

Y.3520

ITU-T Y.4906 5G

5G [4] ITU-T F.748.46

Re i emen and e al a i n me h d f a ificial

in elligence agen ba ed n la ge cale e- ained m del

ITU-T X.S-A1A Sec i Re i emen and G ideline f! A ificial In elligence Agen

ITU-T X. -ai Sec i e i emen f! AI em

ITU-T X. gGenAI Sec i G ideline f! Gene a i e A ificial In elligence A lica i!n Se ice

ITU-T TR. e-ai Sec i E al a i!n !n A ificial In elligence echn!l!g in ICT

ITU-T X. - aima Sec i e i emen f! e minal-ba ed a ificial in elligence m l i-agen em

ITU-T X.ga d-ma G ideline f! a lica i!n lne abili de ec i!n ba ed !n m l i-agen em

ITU-T TR. em-AIA Sec i e al a i!n me h!d f! an a ificial in elligence agen

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

IEEE P7000 IEEE 7000

IEEE 7000.1

IEEE 7003

IEEE P7000

IEEE P7000.1

IEEE P7000.2

IEEE P7000.3

IEEE P7000.4

IEEE P7005

IEEE P2790

(4)

IEC ISO

ITU 2025 12

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

AI

2.2.2

TC260 TC28 TC260

TC28

[23]

(1)

3 [21] 1

TC260

GB/T 35291-2017

GB/T 38632-2020

2

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

3

TC260

2.0 GB 45438-2025

[24]

2019 [25]

2023 [26]

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

TC2 003

GB/T 42888-2023

GB 45438-2025

M

GB/T 45694-2025 4 æû

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

(2)

2018 [27]

2021 [28]

[29]

[30]

AI

GB/T 41867-2022

GB/T 42018-2022

GB/T 42755-2023

GB/Z 42759-2023

GB/T 43782 2024

2

3

4

5

6

7

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
TC260 Cybersecurity

1

AI

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
全国网络安全标准化技术委员会 TC260 Cybersecurity

AI

3.1

AI

AI

AI

AI

AI

AI

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

会员
of SAC

3.2

3.2.1

1 OWASP O en Web A lica i n Sec i P jec

Web

T 10 f LLM A & Gen AI Agen ic Sec i

Ini ia i e OWASP T 10 f Agen [31]

- T6 T7

  T8

- T1 T5
- T2 T3 T4

  T11

- T9
- T10 T15
- T12 T13 T14

2

2025 9 15

2.0

●

●

●

3 IIFAA

2025 7 28 2025 [32]

●

●

● AI

4 360 2025 7

[33]

20

Gi H b

●

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

-
-

3.2.2

(1)

-
-

(2)

-
-
-
-

(3)

-

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
TC260 Cybersecurity

-

(4)

-

-

-

3.2.3

AIA01 AIA05

11

5

AIA01		/
AIA02		
AIA03		
AIA04		
AIA05		
AIA06		

AIA07		
AIA08		
AIA09		
AIA10		RAG
AIA11		

1.

- AIA02
- AIA03
- AIA04
- AIA05
- AIA07

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

- AIA11

2.

- AIA01

- AIA04
- AIA06
- AIA10

3.3

2 11

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

AIA02 AIA03 AIA04 AIA09

AIA01 AIA02 AIA10 AIA05

AIA11 AIA06 AIA07

AIA08

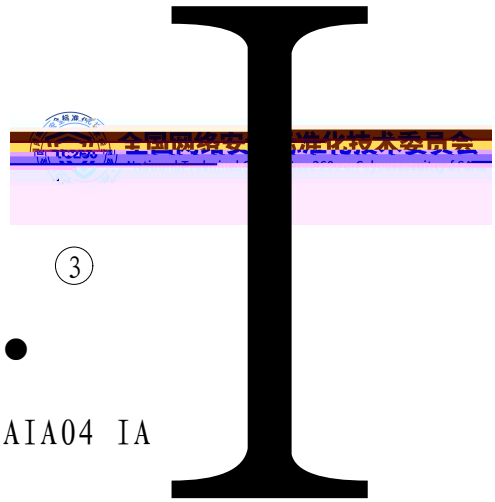
3.3.1

AIA02

- ①
- ②
- ③
- AIA03

- ①
- ②

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC



③

●

AIA04 IA

●

① IA4

②

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

AIA10

- RAG
-
-

2

AIA01

-
-

3

AIA05

-
-

4

AIA11

-
- API

2.

AIA06

-
-

AIA07

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

-
-

3.

AIA08

-
-

3.3.3

6

AIA01			+
AIA10			+
AIA07			+
AIA11			+
AIA05			+

AIA06

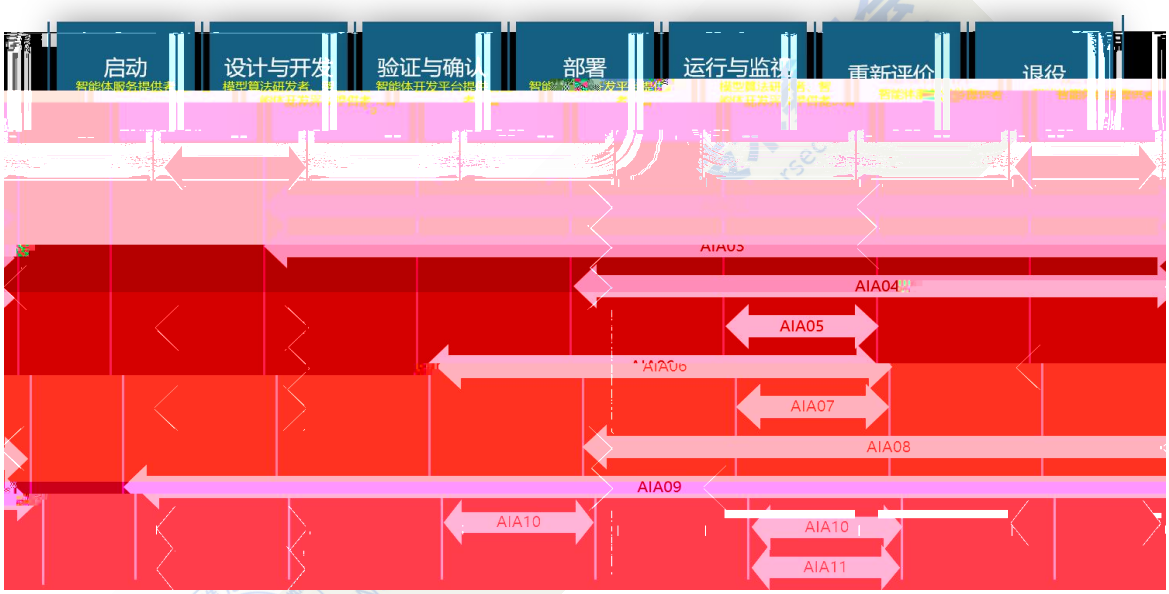
- /

-
-
-

3.4

ISO/IEC 22989

3



3

1)

AIA09

2)

AIA02 AI

AIA03

API

Agen

3)

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

AI

AI

AIA01 AIA10

AI

AIA06

4)

AIA04

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
全国网络安全标准化技术委员会 TC260 Cybersecurity

API

5)

AIA01

AI

AI

AIA05

AIA11

API

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

AIA06

CPU

AIA10

AI

6)

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

AI

7)

AI

AIA02

GAI

7

	AIA09	

	AIA02 AIA03 AIA09	
	AIA01 AIA02 AIA03 AIA06 AIA09 AIA10	
	AIA02 AIA03 AIA04 AIA06 AIA08 AIA09	
	AIA01 AIA02 AIA03 AIA04 AIA05 AIA06 AIA07 AIA08 AIA09 AIA10 AIA11	
/	AIA02 AIA03 AIA04 AIA08 AIA09	

3.5

(1)

-

-

-

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

-

(2)

(3)

(4)

-
-
-
-

(5)

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

-
-

3.2

8

AIA01	
AIA02	

AIA03	
AIA04	
AIA05	
AIA06	

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

AIA07	
AIA08	
AIA09	
AIA10	
AIA11	

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

1.

- AIA04
- AIA07
- AIA11
- AIA02

2.

- AIA01
- AIA04
- AIA06

3.6

1

AIA03 AIA04 AIA07 AIA08 AIA11

2

AIA02 AIA06 AIA09

3

AIA01 AIA05 AIA10

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

4.1

(1)

/

(2)

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

(3)

(4)

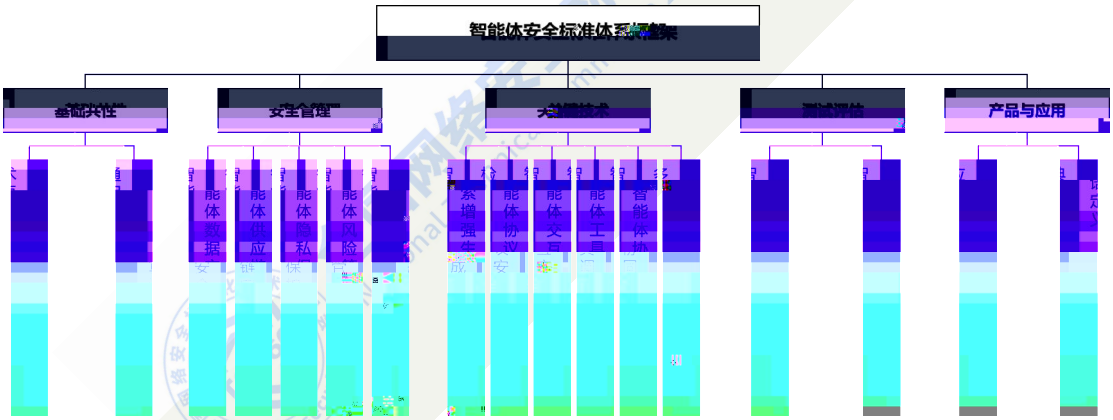
RAG RAG

(5)

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

4.2

4



4

5

(1)

●

-

(2)

-

-

-

-

-

(3)

-

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

-

- A2A ANP MCP

-

-

-

(4)

-

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

-

(5)

-

-

4.3

(1)

GB/T 41867-2022

全国网络安全标准化技术委员会

(2)

GB/T 46351-2025

GB/T 42888-2023

GB/T 45225-2025

GB/T 45652-2025

GB/T 45674-2025

GB/T 42755-2023

ISO/IEC 8183:2023

GB/T 44588-2024

GB/T 46347-2025

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
TC260 Cybersecurity

(3)

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

(4)

(5)

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

2024

5.1

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

4

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

AI

9

9

		AIA01 AIA11	
		AIA01 AIA11	
		AIA04 AIA06 AIA07 AIA11	A2A ANP MCP
		AIA01	

		AIA05	
		AIA01 AIA11	AI
		AIA01 AIA11	AI
		AIA03 AIA04 AIA08 AIA09	
		AIA01 AIA11	

5.2

ISO

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

IEC ITU

+

5.3

TC260

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

A2A　MCP

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

1

2

3

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
全国网络安全标准化技术委员会 TC260 Cybersecurity

1. AI agen AIA

a ma ed en i ha en e and e nd i en i nmen and ake ac in achie e i gal .

a ma ed i " e aining a ce em ha , nde ecified ndi in , f nc in i h h man in e en in".

[ISO/IEC 22989:2022[34]]

2. Pe ce in and gni in

The e ce in and gni in m i e f ecgni in, m ehen in, dialg e, gene a in, and ea ning.

[ITU-T F.748.46[35]]

3. Planning

The lanning incl de a k lanning, a k ched ling and a k imi a in.

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

[ITU-T F.748.46]

4. Mem!

The mem! incl de h! - e m mem! and l!ng- e m mem! .

[ITU-T F.748.46]

5. Ac i!n

The ac i!n incl de i al en i!nmen e ec i!n ca abili and eal- ! ld en i!nmen e ec i!n ca abili .

[ITU-T F.748.46]

6. M!del C!n e P! !c!l MCP

The M!del C!n e P! !c!l MCP i an! en ! !c!l ha enable eamle in eg a i!n be een LLM a lica i!n and e e nal da a ! ce and !!l .

MCP

LLM

[The !fficial ecifica i!n, d!c men a i!n and im lemen a i!n f! he M!del C!n e P! !c!l MCP [36]]

7. Ann! ncing he Agen 2Agen

P ! !c!1 A2A

The Agen 2Agen A2A P ! !c!1 i an ! en anda d de igned ! enable eamle c!mm nica i!n and c!llab! a i!n be een AI agen . In a ! ld he e agen a e b il ing di e e f ame ! k and b diffe en end! , A2A ! ide a c!mm!n lang age, b eaking d! n il! and f! e ing in e ! e abili .

Agen 2Agen A2A

A2A

[Ann! ncing he Agen 2Agen P ! !c!1 A2A [37]]

8. Agen Ne ! k P ! !c!1 ANP

Agen Ne ! k P ! !c!1 ANP

ANP AI

ANP

[Agen Ne ! k P ! !c!1 [38]]

9. !!1

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

B.1

ISO/IEC 22989:2022	Inf ma i n echn l g A ificial in elligence A ificial in elligence c nce and e min l g	ISO/IEC JTC1/SC42
ISO/IEC 23053:2022	F ame k f A ificial In elligence (AI) S em U ing Machine Lea ning (ML)	ISO/IEC JTC1/SC42
ISO/IEC 24029-1:2021	A ificial In elligence (AI) A e men f he b ne f ne al ne k Pa 1: 0 e ie 1	ISO/IEC JTC1/SC42
ISO/IEC TR 27563:2023	Sec i and i ac be ac ice f AI e ca e AI	ISO/IEC JTC1/SC27
ITU-T F.748.46 e F.TE-AIA	Re i emen and e al a i n me h d f a ificial in elligence agen ba ed n la ge cale e- ained m del	ITU

B.2

GB 45438-2025		TC260
GB/T 45674-2025		TC260
GB/T 45652-2025		TC260
GB/T 45654-2025		TC260

TC260-PG-2025NA		TC260
GB/T 42888-2023		TC260
GB/T 45958-2025		TC260
T/CCSA 800-2026		CCSA

B.3

ISO/IEC 27090	C be ec i cial in elligence G ideline ing ec i h ea and fa n AI em	ISO/IEC JTC1/SC27
ISO/IEC 27091	C be ec i and P i ac A ificial In elligence P i ac ec i n	ISO/IEC JTC1/SC27
ISO/IEC PWI 25240	E al a i n f AI-ba ed Techn l g	ISO/IEC JTC1/SC27
ITU-T X.S-A1A	Sec i Re i emen and G ideline f A ificial In elligence Agen	ITU
ITU-T X. -ai	Sec i e i emen f AI	ITU
ITU-T X. gGenAI	Sec i G ideline f Gene a i e A ificial In elligence A lica i n Se ice	ITU
ITU-T TR.1e-ai	Sec i E al a i n n A ificial In elligence echn l g in ICT	ITU
ITU-T F.AI ebe		

ITU-T X.ga d-ma	G ideline f a lica i n lne abili de ec i n ba ed n m l i-agen em	ITU
ITU-T TR. em-AIA	Sec i e al a i n me h d f an a ificial in elligence agen	ITU
ITU-T B.agai	De ign P inci le f Iden i Managemen (IM) in he C n e f Agen ic AI	ITU
ITU-T TR.1 f-AAI	Land ca e f T F ame k f Agen ic AI AI	ITU

B.4

		TC260
		TC260
	1	TC28/SC42
	2	TC28/SC42
	3	TC28/SC42
	4	TC28/SC42
	5	TC28/SC42
	6	TC28/SC42
	7	TC28/SC42
		TC28/SC42
		TC28/SC42
		TC28/SC42
		TC28/SC42
AI	1	CCSA
		CCSA
		CCSA
		CCSA
		CCSA
		CCSA
		CCSA
		CCSA
		CCSA
		CCSA
		CCSA
		CCSA

	CCSA
	CCSA
	CCSA
	CCSA
	CCSA
	CCSA
	CCSA
RAG	CCSA TC601
	CCSA

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

1.2

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

/

AI C deGeeX AI

Fi en C de Fi en ech

Mic f 365 C il

Sale f ce Ein ein Se iceN AI

/ AI

WPS AI

/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
TC260 Cybersecurity

/

IFTTT

LLM

GPT Cla de Gemini

Agen

Cha b!

Si i/

APP

A !GPT

De in

Man

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

[1] AI Agen Ma ke b Agen R le P d c i i & Pe nal A i an , Sale , Ma ke ing, C me Se ice, C de Gene a i n , Agen S em Single Agen , M l i Agen , P d c T e Read De l Agen , B ild Y O n Agen - Gl bal F eca 2030 [R]. Ma ke and Ma ke , 2024.
[2] . AI Inde Re 2025 [R]. 2025.
[3] . AI [Z]. 2023.
[4] . [Z]. 2024.
[5] . [Z]. .
[6] . AIDA [Z]. .
[7] . [Z]. 2023.
[8] . [Z]. 2024.
[9] . AI [Z]. 2024.
[10] . [Z]. 2017.
[11] . [Z]. 2016.
[12] . [Z]. 2021.
[13] . [Z]. 2021.
[14] . [Z]. 2021.
[15] . [Z]. 2022.
[16] . [Z]. 2021.
[17] . [Z]. 2023.
[18] . [Z]. 2024.
[19] . + [Z]. 2025.
[20] . 2.0

[Z]. 2025.
[21] . [J].
, 2025 04 :69-75.
[22] . [C]// .
2022 . 2022.
[23] .
[J]. , 2023 9 :11-15.
[24] .
V1.0 [Z].2025.
[25] 360
. 2019 [R/OL].
2019.
h :// . c260.! g.cn/ ! a1/a icle/1/2019103115165
.
[2 .
2023 [R/OL]. 2023.
h :// . c260.! g.cn/ ! a1/a icle/2/2023053110515
9.
[ ] .
2018 [R/OL]. 2018.
h :// .ce i.cn/201801/3545.h ml.
[28] .
2021 [R/OL]. 2021.
h :// .ce i.cn/202107/7796.h ml.
[29] .
[R/OL]. 2019.
h :// .ce i.cn/image /edi ! /20190425/201904251426
32634001. df.
[30] .
[R/OL]. 2019.
h :// .ce i.cn/image /edi ! /20190425/201904251431
08915001. df.
[31] OWASP. OWASP T! 10 f! LLM A & Gen AI Agen ic Sec i
Ini ia i e [R/OL]. 2025.
[32] . 2025 [R]. 2025.
[33] 360 .

[34] In e na i nal O gani a i n f
S anda di a i n/In e na i nal Elec l echnical
C mmi i n. Inf ma i n echn l g - A ificial
in elligence - A ificial in elligence c nce and
e min l g : ISO/IEC 22989:2022 [S]. 2022.
[35] In e na i nal Telec mm nica i n Uni n Telec mm nica i n
S anda di a i n Sec l . F nc i nal f ame l k and
ca abili ie l f a ificial in elligence enabled
ne l king: ITU-T F.748.46 [S]. 2023.
[36] M del C n e P l c l. The fficial ecifica i n,
d c men a i n and im lemen a i n f he M del C n e
P l c l MCP [EB/OL]. 2025.
h ://m delc n e l c l. i /.
[37] G gle. Ann ncing he Agen 2Agen P l c l A2A
[EB/OL]. 2025.
h ://de el e .g gleb l g.c m/en/a2a-a-ne -e a- f-a
gen -in e l e abili /.
[38] Agen Ne l k P l c l [R]. ANP , 2024.

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC
TC260 Cybersecurity