Crosswalk Between NIST AI Risk Management Framework (AI RMF 1.0) and TTA Guidebook for Development of Trustworthy AI 2023 – General Sector

December 2024

This document provides a comparative analysis between the Telecommunications Technology Association's (TTA) "Guidebook for Development of Trustworthy AI 2023 - General Sector"* and the National Institute of Standards and Technology's (NIST) "AI Risk Management Framework (RMF)." It provides users of these two documents with the ability to navigate and manage AI risks from two perspectives:

Mapping Subcategories of the NIST AI RMF for each TTA Guidebook Verification Item: this version links the relevant NIST AI RMF subcategories to each of the 67 verification items addressed in the TTA Guidebook. Details are provided on pages 2–8 of this document.

Mapping Verification Items of the TTA Guidebook for each NIST AI RMF Subcategory: conversely, this version links the relevant TTA Guidebook verification items to each of the 72 subcategories of the NIST AI RMF. Details are provided on pages 9–16 of this document.

* The TTA Guidebook is intended to provide practical guidance for developing trustworthy AI products and services. It includes an overview of trustworthiness, global trends, a trustworthiness framework, technical requirements for practitioners, verification items, stakeholders, and a glossary. For inquiries related to this document or the Guidebook, please contact the Center for AI Trustworthiness at TTA. (pentarous@tta.or.kr, yepp1252@tta.or.kr)

Detailed Comparison

Mapping Subcategories of the NIST AI RMF for each TTA Guidebook Verification Item

#	TTA Guidebook Identifier	TTA Guidebook Verification Items	Relevant NIST AI RMF Subcategories
	(Requirement 01) Risk management plan for AI system and execution of the plan		
	(Requirement 01-1) Have you analyzed risk factors that may arise throughout the life cycle of the AI system?		
1	01-1a	Have you identified the risk factors of the AI system and the ripple effect?	MAP 3.2, 5.1 MEASURE 3.1 MANAGE 1.2, 2.3
	(Requirement 01-2) Have you prepared measures to remove and prevent risk factors or mitigate the effects?		
2	01-2a	Have you developed measures to remove risk factors and confirmed if the ripple effects were mitigated?	GOVERN 5.1* MANAGE 1.3, 2.1
	(Requirement 02) Organization of an AI governance system		
	(Requirement 02-1) Have you established guidelines and policies on AI governance?		
3	02-1a	Have you prepared internal guidelines and policies on AI governance?	GOVERN 1.1, 1.4, 2.1, 5.1*, 6.1* MAP 3.5
	(Requirement 02-2) Have you formed an AI governance group and reviewed the composition of the group?		
4	02-2a	Have you formed an AI governance group?	GOVERN 1.2, 1.5
5	02-2b	Is the AI governance group composed of adequately trained members?	GOVERN 2.2, 3.1 MAP 1.2 MEASURE 1.3
	(Requirement 02-3) Is the AI governance being supervised to ensure proper implementation?		
6	02-3a	Is compliance with internal guidelines and policies on AI governance being overseen?	GOVERN 2.3
	(Requirement 02-4) Has the AI governance group reviewed the differences between the new and previous systems?		
7	02-4a	Have you analyzed if the system can be implemented by improving, integrating, or abolishing other infrequently used systems?	MANAGE 2.4

* In this case the TTA Guidebook verification item is a subset of the identified, broader NIST AI RMF subcategory and they are linked here, but they are not linked in the second crosswalk.

continued

#	TTA Guidebook Identifier	TTA Guidebook Verification Items	Relevant NIST AI RMF Subcategories
	(Requirement 03) Development of a plan to test trustworthiness in the AI system		
	(Requirement 03-1) Have you designed a test environment in consideration of the AI system's features?		
8	03-1a	Have you considered the operating environment of the AI system when determining the test environment?	MAP 2.3
9	03-1b	Have you obtained a simulator if the AI system needs a virtual test environment?	MEASURE 2.5, 2.6
	(Requirement 03-2) Have you organized a negotiation system to design the test for the AI system?		
10	03-2a	Have you organized a negotiation system to determine the expected output of the AI system?	GOVERN 5.1 MEASURE 1.3
11	03-2b	Have you organized a user review group to check if the AI system is explainable and interpretable?	GOVERN 5.1, 5.2 MAP 1.6 MEASURE 1.3, 4.2
	(Requirement 04) Provision of detailed information for data utilization		
	(Requirement 04-1) Is there detailed information to support the accurate comprehension and utilization of data?		
12	04-1a	Have you explained the data attributes before and after cleansing?	MAP 2.2
13	04-1b	Have you sorted data into training data and metadata and is there a specification document for each of them?	GOVERN 4.2
14	04-1c	Have you explained the reason for selecting the protected attributes and whether they were reflected?	MEASURE 2.10
15	04-1d	Were data labelers trained and have you provided them with work instructions?	GOVERN 2.2
	(Requirement 04-2) Is data provenance documented and managed?		
16	04-2a	Is the dataset provided by a trustworthy provenance?	GOVERN 4.2 MAP 4.1, 4.2 MEASURE 1.1 MANAGE 3.1
17	04-2b	Have you clearly stated the provenance when using an open-source dataset?	MAP 4.1

continued

#	TTA Guidebook Identifier	TTA Guidebook Verification Items	Relevant NIST AI RMF Subcategories
	(Requirement 05) Inspection of abnormal data to ensure data robustness		
	(Requirement 05-1) Have you inspected the detection of abnormal data and their normality?		
18	05-1a	Have you checked any possible errors by visualizing the overall training data distribution?	No equivalent category
19	05-1b	Have you implemented techniques to detect outliers in training data?	MAP 2.3
	(Requirement 05-2) Have you devised measures to defend against data-oriented attacks?		
20	05-2a	Have you prepared measures to defend against poisoning and evasion attacks?	MEASURE 2.7
	(Requirement 06) Removal of bias in the collected and processed training data		
	(Requirement 06-1) Have you prepared measures to mitigate bias due to human and physical elements in data collection?		
21	06-1a	Have you implemented procedural and technical measures to eliminate human bias?	MAP 1.2
22	06-1b	Have you used a heterogeneous device to ensure data diversity?	No equivalent category
23	06-1c	Have you examined bias in data that may occur due to hardware?	GOVERN 6.1 MANAGE 3.1
	(Requirement 06-2) Have you analyzed features used in training and prepared selection criteria?		
24	06-2a	Have you made a thorough analysis when selecting the protected attributes?	MEASURE 2.10
25	06-2b	Have you mitigated the impact of features that may create bias?	MEASURE 2.11
26	06-2c	Have you reviewed whether features were removed excessively during data pre-processing?	No equivalent category
	(Requirement 06-3) Have you checked and prevented potential biased in data labeling?		
27	06-3a	Have you clearly established the data labeling standards and provided them to labelers?	MAP 2.3
28	06-3b	Have you made an effort to recruit diverse data labelers?	MAP 1.2
29	06-3c	Have you made an effort to recruit diverse reviewers for labeled data?	MAP 1.2
	(Requirement 06-4) Have you conducted sampling to prevent bias in data?		
30	06-4a	Have you implemented a sampling method to prevent bias?	MEASURE 2.11

continued

#	TTA Guidebook Identifier	TTA Guidebook Verification Items	Relevant NIST AI RMF Subcategories
	(Requirement 07) Ensuring security and compatibility of the open–source library		
	(Requirement 07–1) Have you confirmed the stability of the open–source library?		
31	07–1a	Have you used an active open–source library?	MAP 4.1
	(Requirement 07–2) Are you managing the risk factors of the open–source library?		
32	07–2a	Have you fulfilled the license compliance of the open–source library in use?	GOVERN 6.1 MAP 4.1
33	07–2b	Have you confirmed the compatibility and vulnerability of the open–source library in use?	MAP 4.1 MANAGE 3.1
	(Requirement 08) Removal of bias in the AI model		
	(Requirement 08–1) Have you implemented techniques to remove bias in the AI model?		
34	08–1a	Have you chosen a bias removal technique appropriate to the model to be developed?	MEASURE 2.11
35	08–1b	Have you selected quantitative indicators to evaluate and monitor bias and are you managing them?	MEASURE 2.11
	(Requirement 09) Establishment of defensive measures for AI model attacks		
	(Requirement 09–1) Do you have a defense technique in place against model extraction attacks?		
36	09–1a	Have you implemented a defense technique to prepare for model extraction attacks?	MEASURE 2.7
	(Requirement 09–2) Do you have a defense technique in place against model evasion attacks?		
37	09–2a	Have you implemented a defense technique to prepare for model evasion attacks?	MEASURE 2.7
	(Requirement 10) Explanation of AI model specifications and the inference results		
	(Requirement 10–1) Do you provide evidence for users to accept the generation process of the model's inference results?		
38	10–1a	If XAI is applicable, have you reviewed the application of the technique to explain the inference results of the AI model?	MEASURE 2.9
39	10–1b	If XAI is not applicable, have you prepared measures other than the application of the technique?	MEASURE 2.9
	(Requirement 10–2) Have you transparently provided the specification of the model on the AI model specification document?		
40	10–2a	Have you prepared a document that describes the details of the system development process and model operation method?	GOVERN 1.4, 4.3 MEASURE 2.8, 2.9

continued

#	TTA Guidebook Identifier	TTA Guidebook Verification Items	Relevant NIST AI RMF Subcategories
	(Requirement 10-3) When needed, do you provide an explanation about the inference results of the AI model?		
41	10-3a	Have you reviewed whether an explanation of the model's inference result is needed?	MEASURE 2.9
42	10-3b	Have you provided an explanation to users about the inference results of the AI model?	MEASURE 2.9
	(Requirement 11) Removal of potential bias in the implementation of the AI system		
	(Requirement 11-1) Have you made an effort to remove bias due to source code and user interface?		
43	11-1a	Have you examined the possibility of bias in the source code, such as the implementation process of the data access method?	MEASURE 2.11
44	11-1b	Have you examined bias due to the user interface and interaction method?	No equivalent category
	(Requirement 12) Safe mode of AI system and establishment of a process for notification of problems		
	(Requirement 12-1) Have you implemented a safe mode that can respond to problems such as attacks, low performance, and social issues?		
45	12-1a	Have you prepared an exception handling policy for such problems?	GOVERN 6.2 MEASURE 2.8 MANAGE 4.3
46	12-1b	Have you implemented a security technique to reinforce the security of the AI system?	MEASURE 2.7
47	12-1c	Have you considered human intervention if there is a significant ripple effect and high uncertainty due to the AI system's decision-making?	GOVERN 3.2
48	12-1d	Are guidance and action on handling expected user error provided?	MANAGE 4.3
	(Requirement 12-2) Does the system perform the function of alerting the operator if a problem occurs in the AI system?		
49	12-2a	Have you established a notification process for ethical issues such as prejudice and discrimination?	GOVERN 4.3, 5.2* MAP 5.2 MEASURE 3.3, 4.1 MANAGE 4.3
50	12-2b	Have you established a notification process by developing procedures and indicators to evaluate the low system performance?	MEASURE 2.3 MANAGE 2.2, 2.4, 4.2, 4.3

* In this case the TTA Guidebook verification item is a subset of the identified, broader NIST AI RMF subcategory and they are linked here, but they are not linked in the second crosswalk.

continued

#	TTA Guidebook Identifier	TTA Guidebook Verification Items	Relevant NIST AI RMF Subcategories
	(Requirement 13) Improvement of users' comprehension of the explanation of the AI system		
	(Requirement 13-1) Have you analyzed user characteristics and constraints in the AI system?		
51	13-1a	Have you analyzed specific considerations according to the user characteristics?	MEASURE 2.9
	(Requirement 13-2) Have you provided a thorough explanation based on user characteristics?		
52	13-2a	Have you established criteria for the evaluation of explanation according to user characteristics?	MEASURE 2.9
53	13-2b	Have you refrained from using technical terms that are difficult for users to understand?	MEASURE 2.9
54	13-2c	Have you used accurate expressions to lead users to specific behaviors and comprehension?	MEASURE 2.9
55	13-2d	Are the location and timing where an explanation is needed appropriate?	MEASURE 2.9
56	13-2e	Have you utilized various user survey techniques to evaluate user experience?	MEASURE 2.9
	(Requirement 14) Ensuring traceability and modification history of the AI system		
	(Requirement 14-1) Have you established measures to track the AI system's decision-making?		
57	14-1a	Have you developed measures to track the contribution to the AI system's decision-making?	GOVERN 6.1
58	14-1b	Have you put in place the log collection function to track the AI system's decision-making?	MEASURE 2.4
59	14-1c	Do you collect and manage user logs to continuously monitor user experience?	GOVERN 6.1
	(Requirement 14-2) Have you obtained the modification history of training data and managed the impact of data modifications?		
60	14-2a	Have you prepared measures to track the data flow and lineage?	MAP 2.3
61	14-2b	Have you developed measures to monitor modifications in the data source?	MANAGE 3.1
62	14-2c	Have you managed the versions during data change?	MANAGE 4.3
63	14-2d	Do you provide information to stakeholders when data change?	GOVERN 1.4, 4.3
64	14-2e	When new data have been collected, do you reevaluate the performance of the AI model?	MEASURE 4.3

continued

#	TTA Guidebook Identifier	TTA Guidebook Verification Items	Relevant NIST AI RMF Subcategories
	(Requirement 15) Explanation about the scope of services provided and the subject of interactions		
	(Requirement 15–1) Do you provide an explanation to encourage proper usage of the AI service?		
65	15–1a	Do you provide an explanation about the goal and objective of the AI service?	MAP 1.1, 2.2
66	15–1b	Do you provide an explanation about the limitation and scope of the AI service?	GOVERN 4.3 MAP 1.1, 2.2, 3.3 MEASURE 2.5
	(Requirement 15–2) Do you accurately explain the subject of the interaction?		
67	15–2a	Have you accurately explained to users that they are interacting with the AI?	MAP 3.4

Mapping Verification Items of the TTA Guidebook for each NIST AI RMF Subcategory

#	NIST AI RMF Identifier	NIST AI RMF Subcategories	Relevant TTA Guidebook Verification Items
	GOVERN		
	GOVERN 1: Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.		
1	GOVERN 1.1	Legal and regulatory requirements involving AI are understood, managed, and documented.	02–1a
2	GOVERN 1.2	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	02–2a
3	GOVERN 1.3	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	No equivalent item
4	GOVERN 1.4	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.	02–1a 10–2a 14–2d
5	GOVERN 1.5	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	02–2a
6	GOVERN 1.6	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	No equivalent item
7	GOVERN 1.7	Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.	No equivalent item
	GOVERN 2: Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.		
8	GOVERN 2.1	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	02–1a
9	GOVERN 2.2	The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.	02–2b 04–1d
10	GOVERN 2.3	Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.	02–3a

continued

#	NIST AI RMF Identifier	NIST AI RMF Subcategories	Relevant TTA Guidebook Verification Items
	GOVERN 3: Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.		
11	GOVERN 3.1	Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).	02-2b
12	GOVERN 3.2	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.	12-1c
	GOVERN 4: Organizational teams are committed to a culture that considers and communicates AI risk.		
13	GOVERN 4.1	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	No equivalent item
14	GOVERN 4.2	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	04-1b 04-2a
15	GOVERN 4.3	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing.	10-2a 12-2a 14-2d 15-1b
	GOVERN 5: Processes are in place for robust engagement with relevant AI actors.		
16	GOVERN 5.1	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.	03-2a 03-2b
17	GOVERN 5.2	Mechanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation.	03-2b
	GOVERN 6: Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.		
18	GOVERN 6.1	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third-party's intellectual property or other rights.	06-1c 07-2a 14-1a 14-1c
19	GOVERN 6.2	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.	12-1a

continued

#	NIST AI RMF Identifier	NIST AI RMF Subcategories	Relevant TTA Guidebook Verification Items
	MAP		
	MAP 1: Context is established and understood.		
20	MAP 1.1	Intended purposes, potentially beneficial uses, context specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.	15-1a 15-1b
21	MAP 1.2	Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their participation is documented. Opportunities for interdisciplinary collaboration are prioritized.	02-2b 06-1a 06-3b 06-3c
22	MAP 1.3	The organization's mission and relevant goals for AI technology are understood and documented.	No equivalent item
23	MAP 1.4	The business value or context of business use has been clearly defined or - in the case of assessing existing AI systems - re-evaluated.	No equivalent item
24	MAP 1.5	Organizational risk tolerances are determined and documented.	No equivalent item
25	MAP 1.6	System requirements (e.g., "the system shall respect the privacy of its users") are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI risks.	03-2b
	MAP 2: Categorization of the AI system is performed.		
26	MAP 2.1	The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).	No equivalent item
27	MAP 2.2	Information about the AI system's knowledge limits and how system output may be utilized and overseen by humans is documented. Documentation provides sufficient information to assist relevant AI actors when making decisions and taking subsequent actions.	04-1a 15-1a 15-1b
28	MAP 2.3	Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation.	03-1a 05-1b 06-3a 14-2a

continued

#	NIST AI RMF Identifier	NIST AI RMF Subcategories	Relevant TTA Guidebook Verification Items
	MAP 3: AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.		
29	MAP 3.1	Potential benefits of intended AI system functionality and performance are examined and documented.	No equivalent item
30	MAP 3.2	Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness - as connected to organizational risk tolerance - are examined and documented.	01-1a
31	MAP 3.3	Targeted application scope is specified and documented based on the system's capability, established context, and AI system categorization.	15-1b
32	MAP 3.4	Processes for operator and practitioner proficiency with AI system performance and trustworthiness - and relevant technical standards and certifications - are defined, assessed, and documented.	15-2a
33	MAP 3.5	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.	02-1a
	MAP 4: Risks and benefits are mapped for all components of the AI system including third-party software and data.		
34	MAP 4.1	Approaches for mapping AI technology and legal risks of its components - including the use of third-party data or software - are in place, followed, and documented, as are risks of infringement of a third party's intellectual property or other rights.	04-2a 04-2b 07-1a 07-2a 07-2b
35	MAP 4.2	Internal risk controls for components of the AI system, including third-party AI technologies, are identified and documented.	04-2a
	MAP 5: Impacts to individuals, groups, communities, organizations, and society are characterized.		
36	MAP 5.1	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.	01-1a
37	MAP 5.2	Practices and personnel for supporting regular engagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.	12-2a

continued

#	NIST AI RMF Identifier	NIST AI RMF Subcategories	Relevant TTA Guidebook Verification Items
	MEASURE		
	MEASURE 1: Appropriate methods and metrics are identified and applied.		
38	MEASURE 1.1	Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.	04-2a
39	MEASURE 1.2	Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities.	No equivalent item
40	MEASURE 1.3	Internal experts who did not serve as front-line developers for the system and/or independent assessors are involved in regular assessments and updates. Domain experts, users, AI actors external to the team that developed or deployed the AI system, and affected communities are consulted in support of assessments as necessary per organizational risk tolerance.	02-2b 03-2a 03-2b
	MEASURE 2: AI systems are evaluated for trustworthy characteristics.		
41	MEASURE 2.1	Testsets, metrics, and details about the tools used during TEVV are documented.	No equivalent item
42	MEASURE 2.2	Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.	No equivalent item
43	MEASURE 2.3	AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented.	12-2b
44	MEASURE 2.4	The functionality and behavior of the AI system and its components – as identified in the MAP function – are monitored when in production.	14-1b
45	MEASURE 2.5	The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability beyond the conditions under which the technology was developed are documented.	03-1b 15-1b
46	MEASURE 2.6	The AI system is evaluated regularly for safety risks – as identified in the MAP function. The AI system to be deployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics reflect system reliability and robustness, real-time monitoring, and response times for AI system failures.	03-1b

continued

#	NIST AI RMF Identifier	NIST AI RMF Subcategories	Relevant TTA Guidebook Verification Items
47	MEASURE 2.7	AI system security and resilience - as identified in the MAP function - are evaluated and documented.	05–2a 09–1a 09–2a 12–1b
48	MEASURE 2.8	Risks associated with transparency and account ability - as identified in the MAP function – are examined and documented.	10–2a 12–1a
49	MEASURE 2.9	The AI model is explained, validated, and documented, and AI system output is interpreted within its context - as identified in the MAP function - to inform responsible use and governance.	10–1a 10–1b 10–2a 10–3a 10–3b 13–1a 13–2a 13–2b 13–2c 13–2d 13–2e
50	MEASURE 2.10	Privacy risk of the AI system - as identified in the MAP function - is examined and documented.	04–1c 06–2a
51	MEASURE 2.11	Fairness and bias - as identified in the MAP function - are evaluated and results are documented.	06–2b 06–4a 08–1a 08–1b 11–1a
52	MEASURE 2.12	Environmental impact and sustainability of AI model training and management activities - as identified in the MAP function - are assessed and documented.	No equivalent item
53	MEASURE 2.13	Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.	No equivalent item
	MEASURE 3: Mechanisms for tracking identified AI risks over time are in place.		
54	MEASURE 3.1	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	01–1a
55	MEASURE 3.2	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.	No equivalent item
56	MEASURE 3.3	Feedback processes for end users and impacted communities to report problems and appeal system outcomes are established and integrated into AI system evaluation metrics.	12–2a

continued

#	NIST AI RMF Identifier	NIST AI RMF Subcategories	Relevant TTA Guidebook Verification Items
	MEASURE 4: Feedback about efficacy of measurement is gathered and assessed.		
57	MEASURE 4.1	Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented.	12-2a
58	MEASURE 4.2	Measurement results regarding AI system trustworthiness in deployment context(s) and across the AI lifecycle are informed by input from domain experts and relevant AI actors to validate whether the system is performing consistently as intended. Results are documented.	03-2b
59	MEASURE 4.3	Measurable performance improvements or declines based on consultations with relevant AI actors, including affected communities, and field data about context relevant risks and trustworthiness characteristics are identified and documented.	14-2e
	MANAGE		
	MANAGE 1: AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.		
60	MANAGE 1.1	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	No equivalent item
61	MANAGE 1.2	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.	01-1a
62	MANAGE 1.3	Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options can include mitigating, transferring, avoiding, or accepting.	01-2a
63	MANAGE 1.4	Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented.	No equivalent item
	MANAGE 2: Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.		
64	MANAGE 2.1	Resources required to manage AI risks are taken into account - along with viable non-AI alternative systems, approaches, or methods - to reduce the magnitude or likelihood of potential impacts.	01-2a
65	MANAGE 2.2	Mechanisms are in place and applied to sustain the value of deployed AI systems.	12-2b
66	MANAGE 2.3	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	01-1a

continued

#	NIST AI RMF Identifier	NIST AI RMF Subcategories	Relevant TTA Guidebook Verification Items
67	MANAGE 2.4	Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.	02-4a 12-2b
	MANAGE 3: AI risks and benefits from third-party entities are managed.		
68	MANAGE 3.1	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	04-2a 06-1c 07-2b 14-2b
69	MANAGE 3.2	Pre-trained models which are used for development are monitored as part of AI system regular monitoring and maintenance.	No equivalent item
	MANAGE 4: Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.		
70	MANAGE 4.1	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.	No equivalent item
71	MANAGE 4.2	Measurable activities for continual improvements are integrated into AI system updates and include regular engagement with interested parties, including relevant AI actors.	12-2b
72	MANAGE 4.3	Incidents and errors are communicated to relevant AI actors, including affected communities. Processes for tracking, responding to, and recovering from incidents and errors are followed and documented.	12-1a 12-1d 12-2a 12-2b 14-2c

Acknowledgment

This work was supported by the Korean MSIT (Ministry of Science and ICT) as Establishing the foundation of AI Trustworthiness (TTA). This crosswalk was done in consultation with NIST.

About the TTA Authors

Introduction to the Center for Trustworthy AI

The Center for Trustworthy AI at the Telecommunications Technology Association (TTA) aims to facilitate the safe and trustworthy use of AI through policy research and testing and certification. The center is comprised of the AI Trustworthiness Policy & Research Team and the AI Trustworthiness Certification Team. The AI Trustworthiness Policy & Research Team is engaged in research on a number of topics, including generative AI testing frameworks, risk management methodologies for general-purpose AI, and watermarking technologies for synthetic content. Based on these research outcomes, the team engages in international collaboration and standardization, contributing to a policy think-tank in South Korea. Additionally, the AI Trustworthiness Certification Team operates the Certification of AI Trustworthiness (CAT) program, provides guidance to businesses on relevant matters, and develops tools necessary for verification. The contributions of the Center for Trustworthy AI are invaluable in shaping South Korea’s AI policies and national standards, enhancing the trustworthiness and safety of AI technologies.

Contributor Biographies

Yejin Shin is a principal researcher on the AI Trustworthiness Policy & Research Team at TTA.Dr. Shin is the main editor of the "Guidebook for Development of Trustworthy AI - General Sector" and leads international collaborations with various countries based on the Guidebook. She also contributes to the research on risk management methods for general-purpose AI. (yepp1252@tta.or.kr)

JoonHo Kwak is the team manager of the AI Trustworthiness Policy & Research Team at TTA. With a background in the testing and certification of software systems and software safety engineering, Mr Kwak is currently leading a project aimed at developing the requirements and verification and validation methodologies for trustworthy AI. He is also actively involved in international standardization efforts in the area of AI trustworthiness and is a member of the ISO/IEC JTC1 SC42 committee. (pentarous@tta.or.kr)