



IEEE Standard for the Procurement of Artificial Intelligence and Automated Decision Systems

IEEE Society on Social Implications of Technology

Developed by the
Social Implications of Technology Standards Committee

IEEE Std 3119™-2025

IEEE Standard for the Procurement of Artificial Intelligence and Automated Decision Systems

Developed by the

IEEE SA Standards Board
of the
IEEE Computer Society

Approved 27 March 2025

IEEE SA Standards Board

Abstract: The standard helps procurement teams reduce risks in artificial intelligence systems (AIS) by using tailored risk management practices when purchasing AIS. Specific process steps for AIS problem definition, solicitation preparation, vendor and solution evaluation, contract negotiation, and contract monitoring are described. Risk management methodologies that augment customary activities and tasks performed during the procurement life cycle are provided including identifying, analyzing, evaluating, prioritizing, mitigating, and controlling unique AIS risks that can detract from unique AIS benefits. How procurement teams can use and apply practical AIS tools and metrics is also provided. The standard focuses explicitly on AIS risks (when compared to traditional, non-AIS technology) and is designed to address the purchase of commercial AI products and services procured using a formal contract or contract framework.

Keywords: ADS, AI, AIS, AI performance, AI solution evaluation, AI systems, AI vendor evaluation, artificial intelligence, acquisition, automated decision systems, commercial AI products and services, contract monitoring, contract negotiation, data, data governance, due diligence, high-risk, human rights, IEEE 3119, impact assessment, metrics, procurement, public engagement, public interest, responsible AI, responsible procurement, risk assessment, risk identification, risk management, risk mitigation, sociotechnical, solicitation, systems, technology

NOTE—AI and ADS are referred to as artificial intelligence systems (AIS) for simplicity.

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2025 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 23 May 2025. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-2201-7 STD27936
Print: ISBN 979-8-8557-2202-4 STDPD27936

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all IEEE standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers involved in technical working groups are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning all standards, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or compliance with law, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English language version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. “Artificial intelligence” refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual is not, and shall not be considered or inferred to be, the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE or IEEE SA. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter’s views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s). News releases about IEEE standards issued by entities other than IEEE SA should be considered the view of the entity issuing the release rather than the formal position of IEEE or IEEE SA.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments or questions, except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE SA working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#).¹ An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

¹ Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

² Available at: <https://standards.ieee.org/about/contact/>.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, data privacy, and interference protection practices and all applicable laws and regulations.

³ Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴ Available at: <https://standards.ieee.org/standard/index.html>.

⁵ Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

Participants

At the time this standard was completed, the Procurement of Artificial Intelligence and Automated Decision Systems Working Group had the following membership:

Gisele Waters, *Chair and Technical Editor*
Cari Miller, *Vice Chair*
Mana Sadeghipour, *Secretary*

Chloe Autio
Sarah Clarke
Cynthia Conti-Cook
Grant Fergusson
Andrew Gamino-Cheong
Maria Paz Hermosilla
Merve Hickok

Clara Langevin
Richard Moreno
Cristina Muresan
Roya Pakzad
Annette Reilly
Martin Saerbeck
Renee Sieber

Sara Soubelet
Marwa Soudi
Robert Spence
Werner van Huffel
Ben Winters
Erica Wissolik
Lisa Wymer

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Matias Aranguiz Villagran
Manomit Bal
Kerry Blinco
Pieter Botman
Sharmeela Chenniappan
Mohd Anwar Jamal Faiz
A. Ferraro
Merc Fox
Deborah Hagar
Victoria Hailey
Maria Paz Hermosilla
Werner Hoelzl
Piotr Karocki

Quist-Aphetsi Kester
Ruth Lewis
Weili Liu
Fernando Lucas Rodriguez
Cari Miller
Monique Morrow
Macaulay Osaisai
Sivaraman P
Howard Penrose
George Percivall
Louis Randazzo III
R. K. Rannow
Annette Reilly

Martin Saerbeck
Ricardo Sanz
Robert Schaaf
Jhony Sembiring
Robert Spence
Walter Struppler
Bin Tang
Mahesh Vajjainthymala Krish
Gisele Waters
Stephen Webb
Erik Whiting
Peter Wishart
Aleksander Zadrozny

When the IEEE SA Standards Board approved this standard on 27 March 2025, it had the following membership:

Lei Wang, *Chair*
Jon Walter Rosdahl, *Vice Chair*
David J. Law, *Past Chair*
Alpesh Shah, *Secretary*

Edward Au
Ted Burse
Xiaofeng (Alfred) Chen
Doug Edwards
Nehad El-Sherif
J. Travis Griffith
Deborah Hagar

Guido R. Hiertz
Ronald W. Hotchkiss
Tyler Jaynes
Thomas Koshy
Howard Li
Xiaohui Liu
Kevin W. Lu
Hiroshi Mano

Daleep Mohla
Annette Reilly
Robby Robson
Dan Sabin
F. Keith Waters
Sha Wei
Luyang (Eric) Zhang

Introduction

This introduction is not part of IEEE Std 3119-2025, IEEE Standard for the Procurement of Artificial Intelligence and Automated Decision Systems.

In an era where organizations and governments increasingly turn to AIS to achieve efficiencies, gain new insights, and enhance engagement with staff, customers, and stakeholders, the importance of procuring trustworthy, reliable, explainable, and rights-respecting solutions cannot be overstated. However, while the benefits of AIS appear compelling, they are often accompanied by hidden or unknown risks and unexpected outcomes. These unknown factors can quickly erode and erase the advantages—making it imperative for organizations to adopt due diligence and accountability measures.

Further, unlike traditional technology, AIS exponentially scales these risks to individuals, groups, communities, and even entire jurisdictions. As such, organizations are recognizing the far-reaching impacts their choice of AIS providers and solutions can have on individuals, communities, markets, and economies. With this emergence of opportunity and concurrent risk among liabilities, competing interests, and incentives, it has become imperative for organizations to take a thoughtful approach to procurement that truly considers all of the potential effects. Lastly, focusing on responsible AI design and development or solely on the governance of these AI systems while they are in use has been insufficient to protect the public interest.

This standard addresses these challenges by establishing a comprehensive set of uniform definitions and a series of process steps for the procurement of AIS designed to identify and reduce risks. The risk-based approach set forth in the standard is tailored to the unique complexities of AIS as they differ from traditional non-AIS technologies. With a distinct lens on the needs of deploying and managing AIS responsibly, the standard aims to augment and fortify existing procurement procedures. By adopting IEEE Std 3119, organizations are given the means to navigate these new challenges with a structured, international consensus-based framework.

The scope of IEEE Std 3119 is primarily focused on the procurement of commercial AI products and services (CAIPS). It excludes in-house and hybrid public-private development of AIS, concentrating instead on providing guidance for the responsible procurement of CAIPS within a formal contractual framework. In addition, the processes outlined in the standard are designed to be integrated into existing practices within the procurement life cycle as a whole or used modularly, offering flexibility in implementation.

The IEEE 3119 process model comprises six processes: Problem Definition, Solicitation Preparation, Vendor Evaluation, Solution Evaluation, Contract Negotiation, and Contract Monitoring. These detailed and tooling processes allow organizations to conduct risk-based due diligence efficiently and effectively. Diligence is much needed to verify that the AIS meets organizational needs while concurrently mitigating potential harms to safeguard the interests, rights, and well-being of all stakeholders involved. Ultimately, organizations can use IEEE Std 3119 to support the responsible and safe procurement of AIS and foster trust and accountability in using this transformative technology.

Acknowledgments

Permissions have been granted as follows:

- The content in the Risk Appetite Tool in Annex E is reproduced with modification from Miller, C. L. & Waters, G. (2024). Risk Management Framework for the Procurement of Artificial Intelligence (RMF PAIS 1.0): 5.0 Step 1: Risk Appetite (p. 11) with permission from the AI Procurement Lab and Center for Inclusive Change.

- The content in the AI Governance Trigger Points Guide in Annex L is reproduced with modifications from “AI governance triggers: When to act and why it matters” [white paper] with permission from Trustible.
- The content in the AIS Auditing Overview Guide in Annex M is reprinted from *AI Assurance and Auditing: A Brief Overview Guide* with permission from Center for Inclusive Change, ©2024
- The Vendor AI Governance Maturity Assessment, Rubric, and Risk Profile Scoring content in Annex N is reprinted from Miller, C. L. (2023). *Assessing AI Governance Maturity* with permission from the Center for Inclusive Change.

Contents

1. Overview	14
1.1 Scope	14
1.2 Purpose	14
1.3 Applicability and constraints	15
1.4 Overview of the six processes	19
1.5 Word usage	20
2. Normative references	20
3. Definitions, acronyms, and abbreviations	20
3.1 Definitions	20
3.2 Acronyms and abbreviations	30
4. Conformance	30
5. Key concepts	31
5.1 Guiding principles	31
5.2 Adoption flexibility	32
5.3 Interdisciplinary procurement teams	32
5.4 Stakeholder engagement	32
5.5 Human in the loop	33
5.6 Key roles in AIS procurement teams	33
5.7 Procurement team competency	35
6. Problem Definition Process	36
6.1 Purpose and scope of the process	36
6.2 Outcomes	36
6.3 Activities and tasks	37
6.4 Inputs	39
6.5 Outputs	39
7. Solicitation Preparation Process	39
7.1 Purpose and scope of the process	39
7.2 Outcomes	39
7.3 Activities and tasks	40
7.4 Inputs	42
7.5 Outputs	42
8. Vendor Evaluation Process	42
8.1 Purpose and scope of the process	42
8.2 Outcomes	43
8.3 Activities and tasks	43
8.4 Inputs	44
8.5 Outputs	45
9. Solution Evaluation Process	45
9.1 Purpose and scope of the process	45
9.2 Outcomes	45
9.3 Activities and tasks	45
9.4 Inputs	46
9.5 Outputs	46

10. Contract Negotiation Process	47
10.1 Purpose and scope of the process	47
10.2 Outcomes	47
10.3 Activities and tasks	47
10.4 Inputs	48
10.5 Outputs	49
11. Contract Monitoring Process	49
11.1 Purpose and scope of the process	49
11.2 Outcomes	49
11.3 Activities and tasks	50
11.4 Inputs	53
11.5 Outputs	53
Annex A (informative) Relationship of processes in IEEE Std 3119 to processes in ISO/IEC 42001:2023	55
A.1 Purpose	55
A.2 IEEE Std 3119 to ISO/IEC 42001:2023 cross map	55
A.3 Related standards	56
Annex B (informative) Problem Analysis Tool.....	57
B.1 Purpose.....	57
B.2 Prerequisites.....	57
B.3 Overview of the problem identification approach.....	57
B.4 Worksheet section	58
Annex C (informative) Public identification and engagement guide	60
C.1 Purpose.....	60
C.2 Stakeholder identification, evaluation, and preparation	60
C.3 Gathering stakeholder feedback	61
C.4 Stakeholder feedback assessment	62
Annex D (informative) AI impact assessment and global index	63
D.1 Background.....	63
D.2 Purpose and activities	64
Annex E (normative) Risk Appetite Tool.....	67
E.1 Purpose.....	67
E.2 Key risk indicators	68
E.3 Risk appetite scorecard overview	69
E.4 Population impact dimension	69
E.5 AI system complexity dimension	70
E.6 Risk appetite scorecard template.....	72
E.7 Risk appetite matrix	75
E.8 Interpreting the quadrants.....	76
E.9 Risk appetite 2x2 quadrant matrix examples.....	77
E.10 Risk appetite statements explained.....	79
E.11 Risk appetite statement templates	79
Annex F (informative) Solicitation requirements considerations guidelines.....	81
F.1 Purpose	81
F.2 Usage adaptations	81
F.3 AI risk management topics	81
Annex G (normative) Vendor governance assessment solicitation questions	87
G.1 Purpose	87

G.2 Solicitation preparation instructions	87
G.3 Organizational AI Governance Assessment questions	88
G.4 Organizational AI Governance Assessment scoring rubric	88
Annex H (normative) Solution evaluation questions.....	94
H.1 Purpose	94
H.2 Solicitation preparation instructions	94
H.3 Solution evaluation questions	94
H.4 Additional context for questions.....	98
Annex I (informative) AIS Contract Language Reference Guide	104
I.1 Purpose.....	104
I.2 Full-text reference resources	104
I.3 Categories and intent of AIS-specific contract clauses	105
I.4 Limitations	106
Annex J (normative) Risk Management Schedule	108
J.1 Purpose.....	108
J.2 Risk Management Schedule Template	108
Annex K (informative) AIS Risk Management Metrics Guide	113
K.1 Purpose	113
K.2 Understanding AIS metrics.....	113
K.3 Common AIS monitoring metrics.....	115
K.4 Limitations.....	118
Annex L (informative) AI Governance Trigger Points Guide.....	119
L.1 Purpose.....	119
L.2 Instructions.....	119
L.3 Trigger event classification labels	119
L.4 Trigger event examples	120
L.5 Trigger event responses.....	122
Annex M (informative) AIS Auditing Overview Guide.....	124
M.1 Purpose.....	124
M.2 Why validate an AIS?	124
M.3 Ways to validate an AIS.....	124
M.4 Who should validate an AIS?.....	125
M.5 AIS audit best practices.....	125
M.6 Further reading.....	125
Annex N (normative) AI Governance Maturity Scoring Guide	127
N.1 Purpose	127
N.2 Instructions	127
N.3 Evaluation and scoring tools.....	128
Annex O (normative) Procurement Risk Register (PRR).....	135
O.1 Purpose	135
O.2 Instructions	135
O.3 Procurement Risk Register Template	135
Annex P (informative) Solution evaluation guidelines.....	138
P.1 Purpose	138
P.2 Instruction.....	138

Annex Q (informative) AIS types and use case evaluation supplement.....	144
Q.1 Purpose	144
Q.2 Overview of AIS types	144
Q.3 Use case examples	146
Annex R (normative) AIS Monitoring and Assurance Plan Template	154
R.1 Purpose.....	154
R.2 Instructions.....	154
R.3 Implementation checklist	154
R.4 Obligations Register.....	156
R.5 Third-Party Value Chain Register.....	157
R.6 Risk Monitoring Register	158
R.7 Metrics and Measurements Register	160
R.8 Responsible, accountable, consulted, and informed (RACI) matrix	161
R.9 AIS Change Register.....	162
R.10 Adverse Incident Register.....	163
R.11 Trigger Point Breach Register.....	165
R.12 Decommissioning task checklist.....	166
Annex S (informative) Bibliography	169

IEEE Standard for the Procurement of Artificial Intelligence and Automated Decision Systems

1. Overview

1.1 Scope

The standard establishes a uniform set of definitions and a process model for the procurement of Artificial Intelligence Systems (AIS) and Automated Decision Systems (ADS) by which government entities can address socio-technical and responsible innovation considerations to serve the public interest. The process requirements include the framing of procurement from an IEEE Ethically Aligned Design (EAD) [B28]⁶ foundation and a participatory approach that redefines traditional stages of procurement, such as: problem definition, solicitation preparation, vendor evaluation, solution evaluation, contract negotiation, and contract monitoring. The scope of the standard only addresses the procurement of commercial AIS products and services (CAIPS). This standard does not give specific guidance on in-house AIS development or hybrid AIS public-private development between buyers and sellers. Nor does the standard provide guidance to procurement teams seeking to use AIS as a buying tool that supports the duties and responsibilities of the procurement job function.

1.2 Purpose

The purpose of this standard is as follows:

- a) To establish a uniform set of definitions and process requirements that address the socio-technical and responsible innovation challenges in the procurement of AI/ADS
- b) To support organizations adapting their processes for procuring AI systems responsibly for the public interest
- c) To promote ethically aligned values and robust public engagement in the process model

⁶ Numbers in brackets correspond to the references in Annex S.

1.3 Applicability and constraints

1.3.1 Augmenting traditional procurement practices

This standard augments existing procurement practices with “meaningful transparency” that improves communication about AIS risks, harms, and benefits (Sloane, et al. [B77]). Transparency is one of the primary principles behind this standard. With meaningful transparency, it should be possible, prior to signing a contract that procures AIS, to understand why and how (e.g., by what decision-making logic, algorithm, or prediction mechanism) an AIS will behave in a particular deployment context (IEEE Std 7001-2021 [B31]).

The standard should be used in conjunction with traditional procurement processes to add effective risk assurance tactics and measures that minimize the unique risks associated with acquiring and deploying commercial AI products and services.

1.3.2 Leadership commitment to responsible AIS

Procurement is a powerful tactic within an organization’s commitment to responsible AIS governance. IEEE Std 3119 supports organizations that wish to identify ways to use their procurement processes to procure and deploy AIS responsibly. Projects conforming to IEEE Std 3119 should balance management commitments for time and budget constraints with the long-term values of accountability, responsibility, and risk mitigation. To enable this, the commitment of top executives, dedicated resources and budget, and an agile cross-functional procurement team are all needed to successfully implement this standard.

The processes in this standard apply during the pre-procurement, procurement, contracting, and post-procurement stages found in common traditional procurement approaches. When organizations use IEEE Std 3119, it is the procurement officers, project teams, stakeholder groups, and organizational decision-makers who shall determine whether any AIS is fit for purpose in a way that aligns with their respective priorities, constraints, and the organization’s risk appetite.

Each AIS contains unique circumstances, stakeholders, stakeholder dimensions, input/output relationship complexities, intended outcomes, potential benefits, and possible harmful impacts. Thus, each procurement has a unique risk profile, which means the procurement team shall evaluate each procurement carefully by clearly identifying the problem to be solved with an AIS, determining how much risk the organization is willing to “accept” from the vendor(s) they select to deliver the AIS, identify risks and mapping relevant and appropriate proportionate risk mitigations, and ensuring contract clauses and monitoring metrics meet the moment of each use case.

Hence, IEEE Std 3119 enables organizations to critically evaluate AIS through supplemental and responsible AIS procurement processes. Organizations shall use the standard to augment their existing procurement requirements to address the knowledge gaps between uncertain buyers and confident AIS sellers. Without the standard, organizations risk failing to select a diligent approach to mitigate AIS risks in the absence of knowledge, competency, and certainty. These failings unnecessarily limit information obtained in proposals (solicitations), which leads to costly litigation (Electronic Privacy Information Center [B17]), constrains bid evaluations, and erodes negotiation advantages later on in the procurement process (Kahn [B54]). By adopting this standard, organizations are empowered with guidance and tools to require robust disclosure on target AIS to better understand what’s being sold. IEEE Std 3119 raises the standard in how procurement teams worldwide understand what AIS is, what functions it serves, and whether AIS is needed (AlgorithmWatch [B3]).

1.3.3 Procurement team AIS literacy

IEEE Std 3119 only addresses a discrete set of activities and tasks within the procurement life cycle that are particularly prime for identifying and controlling AIS risks. The standard is not meant to be an educational standard that teaches procurement teams basic or advanced AIS literacy. Hence, in addition to understanding the procurement life cycle, procurement teams should bring with them a moderate level of AIS knowledge in order to get the most out of the standard. Ideally, procurement teams will understand basic AIS terminology, types of AIS, the AIS development life cycle, actors within the AIS supply chain, general risks and harms that high-risk AIS include, a basic understanding of how developers test and monitor systems, and general principles of AIS risk governance.

1.3.4 Organizational AIS governance readiness

IEEE Std 3119 provides repeatable process steps to identify and control risks that emanate through vendor actions (e.g., training data integrity, machine learning drift, etc.). IEEE Std 3119 does not address all AIS governance for an entire organization. It is only one governance element of a larger picture. The standard is meant to complement other organizational AIS governance tactics such as responsible AIS policies, policies and processes for data governance, protocols for handling end user appeals when an AIS produces an unfair result, discipline AIS training requirements for new employees, periodic testing AIS explainability with organizational stakeholders, etc. The standard does not provide guidance on these types of other organizational AIS governance needs that, ideally, should be in place in order for an organization to be ready to onboard AIS responsibly.

1.3.5 Key concepts and application

IEEE Std 3119 is oriented toward procurement conducted by government organizations. There are many stakeholders involved in the procurement value chain that can benefit from this standard. It is important that all stakeholders comply with the government's requirements. Therefore, other organizations outside of government entities can also benefit from proactively learning about the transparency requirements found in this standard.

The AI value chain is complex and extensive. This standard is designed as a sector agnostic⁷ and horizontal standard. Its key concepts can be adopted by a wide variety of organizations including AIS vendors, non-profits, private businesses, research organizations, educational institutions, and other types of organizations that may either directly or indirectly require conformance with governmental procurement standards and/or compliance with relevant laws and regulations related to the responsible use of government funds. Proactive leaders in both the public and private sectors, on the buying and selling sides of procurement, can benefit from applying the standard's key concepts.

The six processes in the standard (Clause 6 through Clause 11) are recommended for use by government agencies, private organizations, non-profits, and other non-governmental organizations. All six processes shall be adopted, or individual processes shall be selected as necessary to serve specific functions within a procurement life cycle or to benchmark a particular AIS use case, with either the informative and/or normative guidance and tools.

1.3.6 AIS sustainability assessments

The standard does not provide guidance on evaluating the sustainability impacts of AIS. Given the variability of laws and regulations from jurisdiction to jurisdiction regarding technology sustainability

⁷ The standard is **NOT** meant for use in military or national defense related procurement projects.

requirements, procurement teams should rely on resources outside of IEEE Std 3119 to identify and evaluate AIS opportunities and risks with respect to sustainability.

1.3.7 High-risk AIS domains

IEEE Std 3119 is optimally applied to AIS that are deployed to serve the public interest and/or pose “high-risk” to impacted stakeholders. Some AIS are always considered high-risk, unless they do not pose a significant risk to people’s health, safety, or rights. High-risk AIS are also identified as rights and safety impacting AIS that focus on consequential or critical decisions. It is not the purpose of the IEEE Std 3119 to provide an exhaustive list of rights-impacting or safety-impacting AIS or high-risk AIS. As AIS technology and use cases continue to evolve rapidly, it would be impossible to have a fully comprehensive list of all AIS use cases that could be high-risk and impact rights or safety. Classification of AIS into risk classes is beyond the scope of this standard. The methodology (process model) adopted in IEEE Std 3119 is a streamlined approach, applicable to uses that meet a presumptive “high-risk” threshold, as they significantly impact rights and safety in the following contexts:

- a) Education and vocational training, including, but not limited to, assessment, accreditation, or certification
- b) Employment, worker management or self-employment
- c) Essential utilities such as electricity, heat, water, Internet or telecommunications access or transportation
- d) Family planning services, including, but not limited to, adoption services or reproductive services
- e) Financial services, including, but not limited to, any financial service provided by a mortgage company, and/or from a creditor or mortgage broker
- f) Medical and health care, including, but not limited to, mental health care, dental care, or vision care
- g) Housing or lodging, including, but not limited to, any rental, short-term housing, or lodging
- h) Legal services, including, but not limited to, private mediation or arbitration, law enforcement,
- i) Government benefits
- j) Other relevant public services not aforementioned

1.3.8 Focus on commercial AIS

The standard is based on (but not exclusively) the procurement of AIS that are largely commercial AI products and services (CAIPS) ready for purchase without substantial modifications but may include standard customizations universally available to all customers. Substantial modifications refer to changes in the CAIPS that invalidate previous testing, verification, and validation. The scope also includes these same types of systems when embedded as individual or aggregated components within larger technology platforms and systems (e.g., U.S. state Medicaid eligibility system using an aggregated and AIS-enabled solution determining the terms and conditions of benefits). In other words, this standard shall be more effective in use cases where commercial AI products and services, the context of application, and the stakeholder impacts are clearly identified (*HCAI Framework* [B53]).

1.3.9 Usage with non-commercial AIS

The standard does not give specific guidance on in-house AIS development or hybrid AIS public-private development. That said, the overarching principles and many of the tools in the standard’s annexes can support and inform the development of in-house and hybrid development of AIS. These practical tools will help evaluate, measure, and monitor vendor and developer participants and AIS components. More

specifically, these tools offer novel, useful, and rigorous approaches to identify and document risk across projects.

1.3.10 Evaluating benefits and risks

AIS is commonly sought after for its perceived benefits. Oftentimes, it is difficult to assess the benefits of an AIS. Pilot testing and trial runs are strongly recommended. In the absence of applying AIS to an actual working use case, benefits shall be assessed similarly to risks. However, IEEE Std 3119 is designed as a risk-based standard, which means it focuses on helping procurement teams assess risks. This assumes that procurement teams have alternate means of assessing benefits that they will then weigh against the risks to determine if the AIS will achieve the designed effects once deployed without the risks outweighing the benefits.

1.3.11 Types of procurement contracts

The standard addresses risk mitigation needs at the earliest possible origin of a contract. For example, governments use a wide variety of contract types (e.g., multi-award schedules, government-wide contract frameworks, government-wide contracts, single award contracts, blanket purchase agreements, direct award contracts, Indefinite-Delivery-Indefinite-Quantity contracts, fixed-price contracts, incentive contracts, performance-based contracts, sole source contracts). In some cases, multi-award contracts/frameworks are set up with several vendors, and any organization should use the products and services on that pre-established contract in order to expedite their procurement needs. These cases typically require subsequent buyers to accept and use the terms and conditions that were established during the original contract process. IEEE Std 3119 is designed to address risks and mitigations within the original contract process that was used in order to set up the contract with as many risks minimized as possible. The standard is NOT designed to fulfill the procurement needs of buyers where the contract terms and conditions are already fixed and set.

1.3.12 Procuring AIS vs. using AIS to conduct procurement

The primary focus of this standard is the procurement of commercial AI products and services within a formal contractual framework. IEEE Std 3119 is NOT focused on the use of AIS as a procurement tool (e.g., using generative AIS to evaluate and/or write contract clauses). This standard is ONLY about buying AIS to verify the AIS being purchased has been developed and deployed responsibly.

1.3.13 General limitations

This standard has additional limitations to its scope, as stated in the remainder of this subclause.

The processes described in this standard (Clause 6 through Clause 11) do not prescribe what is ethical, unethical, or what is socially responsible. While the standard is intended to be consistent with the IEEE Code of Ethics [B35], it does not provide ethical guidance for individual procurement managers in their personal judgments regarding their professional work or specific rights or wrongs, nor advice to whistleblowers on how to address gaps and lapses in an organization's capacity to procure AIS responsibly. IEEE Std 3119 is limited to identifying and mitigating risks across the procurement life cycle where AIS outcomes and critical decisions have the potential to impact populations in negative ways, and it is founded on the principles listed in 5.1.

The use of IEEE Std 3119 cannot guarantee that the organization will procure AIS responsibly, nor does this standard "certify" that an organization will procure AIS responsibly. This is a volunteer standard to be used by proactive leaders in organizations that prefer to add risk assurance to their procurement processes.

The nature of each organization's responsibility depends on the capabilities and choices of those who use the standard and the commitment of the organization's hierarchy to full or partial conformance with the standard.

1.4 Overview of the six processes

The primary objectives of IEEE Std 3119 are to guide procurement teams in identifying risks and to establish guardrails that verify commercially-available AIS have been responsibly developed and shall be responsibly deployed. IEEE Std 3119 utilizes six processes (Clause 6 through Clause 11) to establish general instruction (e.g., required activities, tasks, and outcomes) and specific tools (e.g., the annexes) that address six key milestones within the procurement life cycle where AIS risks shall be systematically identified and mitigated with robust diligence.

The six sequential processes are designed to augment and bolster existing procurement practices. They should also be used in a modular fashion to bolster specific functions within a procurement life cycle. The processes cover the following:

- Problem Definition (Clause 6)
- Solicitation Preparation (Clause 7)
- Vendor Evaluation (Clause 8)
- Solution Evaluation (Clause 9)
- Contract Negotiation (Clause 10)
- Contract Monitoring (Clause 11)

Each process offers a detailed set of activities, tasks, tools, templates, rubrics, and more to equip procurement teams (Waters and Miller [B81]) with the elements necessary to identify and mitigate unique risks and challenges in the procurement and deployment of AIS in order to implement AIS responsibly (Hickok [B23]).

For an overview of the procurement life cycle model, refer to Figure 1.

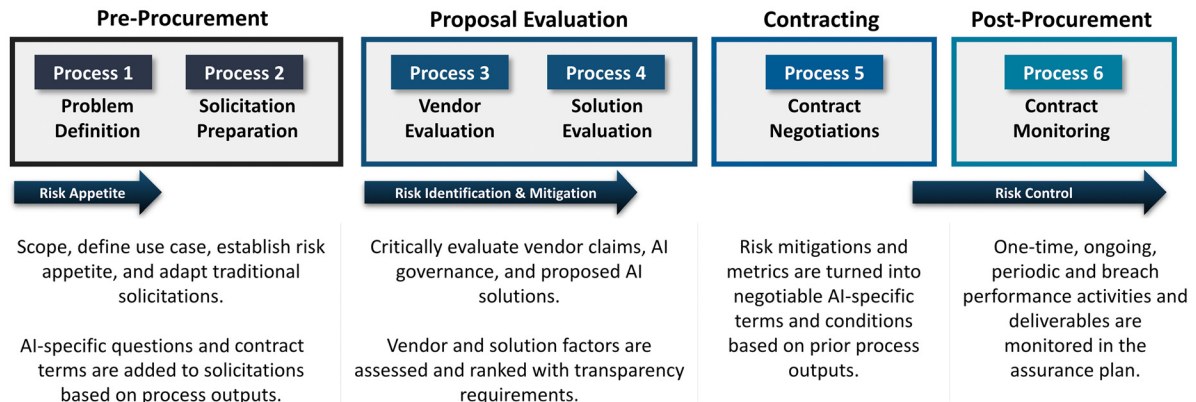


Figure 1—IEEE 3119 processes

1.5 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{8, 9}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

This standard does not require the use of any normative references. Standards useful for the implementation and interpretation of this standard are listed in A.3, Related standards.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms *and definitions apply*. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.¹⁰

NOTE—For additional terms and definitions in the field of systems and software engineering, see ISO/IEC/IEEE 24765:2017 [B47], which is published periodically as a “snapshot” of the SEVOCAB (Systems and Software Engineering Vocabulary) database and is publicly accessible at computer.org/sevocab.¹¹

accountability: Obligation or expectation to control or achieve certain results.

acquisition: The process of purchasing a product, service, or system.

activity: A set of cohesive and purposeful tasks of a process.

adversarial attack: Intrusion into an AI system crafted to deceive and cause the system to make incorrect or unintended predictions or decisions.

agency: Capacity, condition, or state of acting or exerting power.

agreement: Mutual acknowledgment of terms and conditions under which a working relationship is conducted. *See also:* **contract**.

⁸ The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁹ The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

¹⁰ *IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE account is required for access to the dictionary, and one can be created at no charge on the *dictionary sign-in page*.

¹¹ Notes in text and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

algorithm: Sequence of operations that transform an input into an output.

NOTE—See OECD Algorithmic 11 Competition—Background Note [B67].

algorithmic bias: Human bias that arises from technology and failing to recognize and acknowledge potential constraints and/or errors in inputs, models, and/or outputs.

NOTE—Major sources of algorithmic bias are data bias, method bias, societal bias, and output bias.

algorithmic impact assessment (AIA): evaluation of the effect of using an AIS or automated decision system, typically considering duration, reversibility, population, and context impacted.

NOTE—Based on many factors, including systems design, algorithm, data privacy, accuracy, and completeness (data-driven issues), fairness, justice, bias, human rights, or other concerns. The AIA should be used to identify potential negative impacts of using the system and to decide whether to implement the system.

anomalous: Inconsistent with or deviating from the usual, normal, or expected.

architecture: <system> Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution. (IEEE Std 7000-2021)

artificial intelligence (AI): A machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

NOTE 1—Different AIS vary in their levels of autonomy and adaptiveness after deployment (OECD [B66]).

NOTE 2—Inferences can be emergent. AI can be used to make or facilitate a decision or facilitate human decision-making, including to determine the provision of products or services.

artificial intelligence system (AIS): A machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

NOTE—Different AIS vary in their levels of autonomy and adaptiveness after deployment (OECD [B66]).

AI governance: A specific set of roles, responsibilities, policies, and practices intended for the organization to oversee the development, selection, deployment, and use of AIS, to manage associated risks, and help ensure it complies with applicable internal and external requirements and aligns with an organization's objectives.

AI organizational governance maturity: Level in a framework or model used to evaluate the relative status of an organization's AIS governance roles, responsibilities, and policies that guide the responsible development of AIS.

AI organizational readiness: The state of having appropriate people, processes, and platforms in place to incorporate the unique requirements of procuring, deploying, monitoring, and managing AIS responsibly and coherently. This also encompasses factors such as strategy alignment, data assessments and readiness, workforce planning, team skills, and ethical consideration.

NOTE—See Wharton School of the University of Pennsylvania [B82].

audit: Independent examination of a work product or set of work products to assess compliance with specifications, standards, contractual agreements, or other criteria. (ISO/IEC/IEEE 15288:2023)

NOTE—The scope includes professional and industry codes of practice.

automated decision system (ADS)/automated decision making (ADM): A system that aids, supports, or replaces a human decision or estimate of risk or probability.

NOTE 1—Also refers to systems that make final conclusions, decisions, or judgments on behalf of a government jurisdiction or organization without any intervention by an individual acting on behalf of the same (Connecticut General Assembly [B14]).

NOTE 2—These systems use techniques such as rules-based systems, regression, predictive analytics, machine learning, deep learning, and neural nets.

bias: Unfair, unequal, unreasonable, inappropriate, and systematic discrimination against individuals or groups of individuals in favor of others.

NOTE—Intentionally or unintentionally, social bias is embedded in data and algorithms by the developers. Technical bias (algorithmic bias) arises from technology constraints and errors. Emergent bias is an unexpected change in the output data due to changes (learning) by the system.

benefit: Positive outcome that is voluntarily or involuntarily created by a system or process.

NOTE—Benefits correspond to one or more underlying desired values.

buyer: Stakeholder that acquires, purchases, or procures an AIS product or service from a supplier.

NOTE—Other terms commonly used for a buyer are acquirer, customer, deployer, purchaser, or internal/organizational sponsor.

cede: Transfer or delegation (voluntarily or otherwise) of human responsibilities to AIS.

commercial AI products and services (CAIPS): AIS products and services that are ready to be bought and used without substantial modification; may also include standard customizations that are universally available to all customers.

NOTE—Substantial modifications refer to changes in the CAIPS that invalidate previous testing, verification, and validation.

competence: Ability to demonstrate and apply the combination of knowledge, formal and informal skills, training, experience, and behavioral attributes to achieve intended organizational and technical results

NOTE—See IEEE Std 2675-2021 [B29].

consumer: Individual member of the general public, purchasing or using products for private purposes. (ISO Glossary: 2011: Committee for Consumer Policy.)

contract: Single agreement or multi-acquisition framework or schedule that establishes terms and conditions for a contract(s) between a buyer and a seller (also referred to as: agreement, framework, government-wide acquisition, sales agreement, purchase agreement, purchase order, task order, delivery order, operative agreement, etc.).

contract negotiation: Point in the procurement life cycle where the chosen vendor(s) is/are invited to negotiate a set of terms and conditions with a buyer.

contract monitoring: Ongoing oversight and evaluation of the AIS to verify compliance with the agreed terms and conditions defined in the contract.

context of use: Intended operational environment for the AIS including, but not limited to, identified users, operational purpose, inputs, and outputs.

NOTE—The operational environment determines the setting and circumstances of all influences upon a system, including not only other systems, but also people, settings, and social and ecological factors. Ecological factors, however, are beyond the scope of this standard.

control: Ability to determine the nature, sequence, and/or consequences of technical and operational settings, behavior, specific events, and/or experiences.

NOTE—Control includes human control that is being informed by activities; decisional control, having choices over actions; and behavioral control, receiving feedback from actions.

critical decision: Decision or judgment that has any legal, material, or similarly significant (consequential) effect on an individual concerning access to, or the cost, terms, or availability of, including but not limited to, the following: (a) education and vocational training, assessment, accreditation or certification, (b) employment, worker management or self-employment, (c) essential utilities such as electricity, heat, water, Internet or telecommunications access or transportation, (d) family planning services, adoption services or reproductive services, (e) financial services provided by a mortgage company or creditor, (f) health care, mental health care, dental care or vision care, (g) housing or lodging, rental, short-term housing or lodging, (h) legal services, private mediation or arbitration, (i) government benefits, or (j) public services.

NOTE—Connecticut General Assembly [B14].

data consent: Agreement from a data source for the use of their data for specified purposes and duration.

NOTE—Data consent can be revocable or irrevocable, with or without anonymity in the use of the data.

data privacy: Fair and legitimate processing of personal data

NOTE—See IEEE Std 7002-2022 [B32].

dependability: The ability of a system to perform as and when required.

NOTE—A measure of a system’s availability, reliability, and maintainability.

deployer: A natural or legal person, public authority, organization, or other body using an AIS under its authority.

design: (verb) <process> Defines the architecture, system elements, interfaces, and other characteristics of a product, service, or system or system element. (ISO/IEC/IEEE 15288:2015)

NOTE—This definition was modified from ISO/IEC/IEEE 15288:2015 [B44] and added *product* and *service*.)

design: (noun) Result of the design process. (ISO/IEC/IEEE 12207:2017)

discrimination: Make a distinction in favor of or against a person or group, class, or category to which the person belongs rather than according to actual merit or fair, equal, and objective criteria; to show partiality unfairly.

diversity: Representation of the differences in attributes of humans in a group or society or the inclusion of humans with diverse attributes and perspectives in the data, process, systems, and governance of an AI ecosystem.

NOTE—See CSIRO [B5].

drift: Expression of deviation between training data and collected data inputs. (IEEE Std 7014-2024)

NOTE 1—Data drift occurs when data changes after the model is deployed. Each data point exists in a high-dimensional space, which is defined by the number of input features. Data drift occurs when new data points arise from a region of the input space that was less populated by training data.

NOTE 2—Concept drift occurs when the decision boundary changes and is often observed in time-series or streaming data. Concept drift exhibits as deviations to or from the desired system behavior based on some agreed measure of objective fact.

NOTE 3—Algorithmic drift occurs when a change in the system’s processing of the same data results during learning or technical enhancements. This phenomenon leads the system to provide different results when fed the same pre-drift data.

environment: <system> Context determining the setting and circumstances of all influences upon a system. (ISO/IEC/IEEE 42010:2022)

NOTE—Also applies to products and services.

ethical: Conforming to accepted standards of conduct; supporting the realization of positive values or the reduction of negative values.

ethical principle: Shared proposition of ethical values that members of a community can pursue and uphold.

ethical policy statement: High-level declaration endorsed by the top management to explain and demonstrate the organization’s commitment to respect core values in the conduct of its activities.

ethical risk: Risk to ethical values.

ethical value: Value in the context of human culture that supports a judgment on what is right or wrong.

ethics: Branch of knowledge or theory that investigates the correct reasons for thinking that this or that is right.

NOTE—Guidelines for conduct that help people in making a judgment about what is right or wrong.

explainability: <AI> Descriptions, details, and reasons available about/within/through a model or system to make its functioning clear or easy to understand to disparate groups of stakeholders.

NOTE—Explainability can be built into an AIS through its design for stakeholders using the system. It can also be made available through documentation for stakeholders conducting technical audits or other anti-hoc and post hoc system reviews.

explainable AI (XAI): A suite of algorithms for a system that can present the rationale for each successive decision in replicable, reproducible, and predictable ways.

NOTE—XAI can relate to the system inputs or outputs. It is understandable for a specific audience, such as system developers, and not necessarily intended for the public.

fairness: Reasonable, appropriate, and systematic equity in making decisions with an absence of bias and allowing opportunities to individuals or groups of individuals.

government entity: Body, board, department, commission, court, tribunal, authority, organization, or other instrumentality performing public executive, legislative, judicial, legal, administrative, or regulatory functions.

functional requirement: Statement that identifies what results a product or process produces.

harm: (noun) Negative event, social development, circumstance, or series of events resulting in (a) injury or impact to the health of a person or groups of people; (b) disruption of the management and operation of critical infrastructure; (c) violations to human rights or a breach of obligations under the applicable law intended to protect fundamental, labor, and intellectual property rights; (d) damage to property, communities or the environment, or (e) any adverse impact to a human and/or society not already identified.

NOTE 1—Harms correspond to one or more underlying values.

NOTE 2—The focus for IEEE Std 3119 is human-centered risks, harms, and hazards. (OECD [B68]).

harm: (verb) Acting with negative value effects for self or others within a respective AI system or solution, organization, or beyond.

high risk AIS: Any AIS when deployed that makes or is a substantial factor (used to assist) in making (or is capable of altering) the outcome of a critical or consequential decision that could have significant impact on persons, groups, or society.

NOTE—Impact to the health, safety, fundamental rights, or privacy of persons, groups, and/or society as determined directly or indirectly by a risk assessment and/or as designated by local jurisdictional law.

human-centered: Focusing problem-solving, analysis, and design of any activity, product, service, process, or system on humans in their context while seeking to understand and solve the *right* problems to produce positive results that purposefully enhance lives. In contrast to machine-centered where the focus of the same is largely on benefitting from automation through digital ways and means without the necessary full consideration of humans in context.

human rights: Rights to which every person is entitled.

NOTE—Human rights are described in the Universal Declaration of Human Rights (1948), the International Convention on Economic Social and Cultural Rights (1966), and other conventions, treaties, and national laws.

impact assessment: Risk management tool that helps organizations consider the benefits and risks of adopting AI technologies by considering a range of potential impacts.

NOTE—Impact assessments vary based on the type of impact being evaluated and assessed (e.g., fundamental rights impact assessment, data protection impact assessment, algorithmic impact assessment, ethics impact assessment).

incident: Event, circumstance, or series of events where the development, use, or malfunction of one or more AIS directly or indirectly leads to any of the following harms: (a) injury or harm to the health of a person or groups of people; (b) disruption of the management and operation of *critical* infrastructure; (c) violations of human rights or a breach of obligations under the applicable law intended to protect fundamental, labor and intellectual property rights; (d) harm to property, communities, or the environment.

NOTE—See OECD [B68].

life cycle: Framework of processes and activities, from conception through retirement, which are organized into stages, which often function as a common reference for communication and understanding.

model: Representation of a process, device, or concept.

opportunity: Condition or state with the potential to lead to a benefit or gain.

organization: A group of people and facilities with an arrangement of responsibilities, authorities, and relationships.

Example—Corporation, firm, enterprise, government, institution, charity, sole trader, association, or parts or combination thereof.

NOTE—An identified part of an organization (even as small as a single individual) or an identified group of organizations can be regarded as an organization if it has responsibilities, authorities, and relationships. People organized for some specific purpose, such as a club, union, corporation, or society, is an organization.

personal data: Information that is linked or reasonably linkable to an individual natural person.

NOTE 1—In some jurisdictions, this is a legal term; in other jurisdictions, other terms, such as personal information, are used.

NOTE 2—Personal information (PI), personally identifiable information (PII), and Protected health information (PHI) are terms used in some jurisdictions.

problem: Difficulty, uncertainty, or otherwise realized and undesirable event, set of events, condition, or situation that requires investigation and corrective action.

process: A set of interrelated or interacting activities that transform inputs into outputs. (ISO/IEC/IEEE 12207:2017)

process purpose: The high-level objective of performing the process and the likely outcomes of effective implementation of the process.

NOTE—The purpose of implementing the process is to provide benefits to the stakeholders.

procurement: The process of defining scope, timing, and substance of goods and/or services to be supplied; obtaining supplier responses; selecting a supplier; negotiating terms and conditions; awarding a contract; and monitoring the compliance of the system or service delivery with the contract agreement.

NOTE—Procurement can involve financial payment or exchange or sharing of data. Trial use or free use of a service can involve some of the responsibilities of a procured service. Procurement includes activities to advise, plan, obtain, and evaluate goods and services that are used to fulfill stated objectives, obligations, and activities toward desired policy outcomes.

product: The result of a process.

program: Related projects, subprograms, and program activities managed in a coordinated way to obtain benefits not available from managing them individually.

project: Endeavor with defined start and finish criteria undertaken to create a product or service in accordance with specified resources and requirements.

public: Individuals and/or groups of individuals in a community and society.

public interest: concern for the safety and well-being of all people, present and future. *Syn:* **public-sector interest.**

NOTE—Public interest is not limited to people in a specific region or nation.

responsible AI: A framework for developing, deploying, and procuring AI safely and ethically based on the principles of human rights, well-being, accountability, transparency, and awareness of misuse.

NOTE—See Inclusive Change and AI Procurement Lab [B11].

responsibility: Obligation or expectation to perform certain activities with the objective of achieving certain results.

requirement: A statement that translates or expresses a need and its associated constraints and conditions. (ISO/IEC/IEEE 29148:2018)

NOTE—System design needs include system characteristics (such as data flows or data flow characteristics) and system elements.

resource: Asset that is utilized or consumed during the execution of a process. (ISO/IEC/IEEE 12207:2017)

Example—Diverse entities such as funding, personnel, facilities, capital equipment, tools, and utilities such as power, water, fuel, and communication infrastructures.

NOTE—Resources include those that are reusable, renewable, or consumable.

responsible AIS procurement: Establishing an environment of due diligence whereby AIS procurement processes augment traditional approaches to address the unique risks, challenges, and mitigations of AIS.

risk: Effect of uncertainty on objectives and/or a combination of the probability of an event and its consequences. (ISO/IEC/IEEE 16085:2021.)¹²

NOTE 1—An effect is a deviation from the expected—positive or negative. A positive effect is also known as an opportunity.

NOTE 2—Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, and process).

NOTE 3—Risk is often characterized by reference to potential harmful events and consequences, or a combination of these.

NOTE 4—Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

NOTE 5—Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.

risk appetite: The quality and quantity of risk a procurement team determines the organization is willing to “accept” from the vendor(s) they select to deliver the AIS.

NOTE—See Inclusive Changes and AI Procurement Lab [B11].

risk assessment: The overall process of risk identification, risk analysis, and risk evaluation. (ISO 31000:2018)

risk mitigation control: A set of practices and procedures that are put in place based on an organization’s risk appetite to identify and manage potential risks as they emerge throughout the procurement life cycle and manage those risks to provide proper assurance regarding the achievement of intended objectives.

¹² This definition has been modified from its original in ISO/IEC/IEEE 16085:2021 [B46] to include “and/or a combination of a probability of an event and its consequences.”

safety: property of a system such that it does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered. (ISO/IEC TS 5723: 2022)

NOTE—The property of a system includes AIS outputs, which may lead to harmful intended or unintended outcomes.¹³

security: Protection against intentional subversion or forced failure. ((NATO AEP-67)

NOTE—A composite of four attributes—confidentiality, integrity, availability, and accountability—plus aspects of a fifth, usability, all of which have the related issue of their assurance.

service: Performance of activities, work, or duties

NOTE 1—A service is self-contained, coherent, discrete, and can be composed of other services.

NOTE 2—A service is generally an intangible product.

solicitation: A procurement document made available to all interested vendors containing the buyer's requirements for the desired AIS with specific instructions for vendors.

NOTE—*Solicitation* is a key term that has been adopted and used throughout the standard when referring to procurement approaches worldwide [e.g., request for proposals (RFPs), request for quotes (RFQ)s, requests for information (RFI), tenders, bid requests, and framework notice].

stage: Period within the life cycle of an entity that relates to the state of its description or realization.

NOTE 1—Stages relate to major progress and achievement milestones of the entity through its life cycle.

NOTE 2—Stages often overlap.

stakeholder: Individual or organization having a right, share, claim, influence, or interest in a system or in its possession of characteristics that meet their needs and expectations. (ISO/IEC/IEEE 12207:2017)

Example—Human beings using the system, organizations representing human beings using the system, end user, end user organizations, supporters, developers, producers, supplier organizations, trainers, maintainers, disposers, buyers, and regulatory bodies.¹⁴

NOTE—Some stakeholders can have interests that oppose each other or oppose the system.

supplier: An organization or an individual that enters into an agreement with the buyer for the supply of a product or service.

NOTE 1—Other terms commonly used for suppliers are contractors, producers, sellers, or vendors.

NOTE 2—The buyer and the supplier are sometimes part of the same organization.

sustainability: The positive or negative net impact of an AIS on natural resources and greenhouse gas emissions. (ISO/IEC 42001:2023)¹⁵

system: A combination of interacting elements organized to achieve one or more stated purposes (ISO/IEC/IEEE 15288:2015)

¹³ The addition of the note in this definition is a modification of the definition from ISO/IEC TS 5723:2022 [B42].

¹⁴ This definition has been modified from its original in ISO/IEC/IEEE 12207:2017 to include “influence” in the primary definition and “human beings using the system, organizations representing human beings using the system” in the example.

¹⁵ This definition has been modified from its original in ISO/IEC 42001:2023 to include “positive and negative net” and “of an AIS.”

NOTE 1—A system is sometimes considered as a product or as the service it provides.

NOTE 2—In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g., aircraft system. Alternatively, the word “system” is substituted simply by a context-dependent synonym, e.g., aircraft, though this potentially obscures a system principles perspective.

system element: Discrete part of a system that can be implemented to fulfill specified requirements. (ISO/IEC/IEEE 15288:2023)

Example—Hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities or any combination.

task: Required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a process.

third party: A natural or legal person, public authority, organization, or body other than the data recipient/subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

trade-off: Decision-making actions that select from various requirements and alternative solutions on the basis of net benefit to the stakeholders.

transparency: Characteristic of the transfer of information to a stakeholder, which is honest; contains information relevant to the causes of some action, decision, or behavior; and is presented at a level of technicality and in a form that is meaningful to the stakeholder.

trigger: An event that impacts the safety, reliability, ethical, or appropriate use of an AIS, and as a result, requires action(s) by the developer or deployer, which may include documenting the event, providing notifications, correcting the issue, and/or pausing the system.

trustworthy <AI>: Regarded as dependable, safe, and secure across its life cycle by its stakeholders, such as deployers, users, or the public.

use case: Description of the context and variables in which the AIS is operationalized and deployed for a specific applied purpose.

user: Individual or group that interacts with a system or benefits from a system during its utilization. (ISO/IEC 25002:2024)

NOTE—The role of *user* and the role of *operator* are sometimes vested, simultaneously or sequentially, in the same individual or group.¹⁶

validation: confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. (ISO 9000:2015)

NOTE—A system is able to accomplish its intended use, goals, and objectives (i.e., meet stakeholder requirements) in the intended operational environment and the right system was built.¹⁷

value: That which influences the selection from available modes, means, and ends of action.

Examples of positive values—Love, privacy, security, transparency, accountability, generosity, dignity, courage, and fairness.

¹⁶ The addition of the note in this definition is a modification of the definition from ISO/IEC 25002:2024 [B39].

¹⁷ The addition of the note in this definition is a modification of the definition from ISO 9000:2015 [B38].

Examples of negative values—Bias, absence of transparency, absence of privacy, selfishness, and greediness.

NOTE—A value can be positive or negative. A positive value is intuitively recognized because of its relatively high desirability. A negative value is marked by its undesirability.

verification: confirmation, through the provision of objective evidence, specified requirements have been fulfilled. (ISO 9000:2015)

NOTE—Verification is a set of activities that compares a system or system element against the required characteristics. This includes, but is not limited to, specified requirements, design description, and the system itself. The system was built right.¹⁸

3.2 Acronyms and abbreviations

AI	artificial intelligence
AIA	algorithmic impact assessment
AIS	artificial intelligence system
ADS	automated decision system (otherwise known as automated decision-making systems, ADMS)
CAIPS	commercial artificial intelligence products and services
IT	information technology
KPI	key performance indicators
MAP	monitoring and assurance plan
MSA	master services agreement
PRR	Procurement Risk Register
RACI	responsible, accountable, consulted, informed
RFP	request for proposal
SLA	service level agreement
SME	subject matter expert
TEVV	testing, evaluation, verification, and validation

4. Conformance

Options for conformance allow flexibility in the application of this standard. Each process (Clause 6 through Clause 11) has a set of high-level activities and detailed tasks that represent one way to achieve the required outcomes. Users should adopt all processes to help maximize the benefits of the standard. When

¹⁸ The addition of the note in this definition is a modification of the definition from ISO 9000:2015 [B38].

adopted as a whole, users shall assert full conformance to the standard by following all activities and tasks in each process to achieve the required outcomes.

Alternatively, users shall adopt the standard in part. In cases where users already have a superior innovative process variant or AIS risk-reduction procurement technique that achieves proportionately similar or better results to the standard (i.e., or a specific outcome), users should decide not to implement a certain process (or activity) in the standard if the process would be duplicative and/or would yield a lesser outcome. In this case, users should declare the need to use only some processes (or some activities within a process) in the standard. These users shall assert full conformance to the standard by following the process steps to achieve the outcomes declared as needed.

NOTE 1—IEEE/ISO/IEC 24774 [B47] explains the concepts of outcomes, outputs, activities, and tasks.

NOTE 2—IEEE standards cannot guarantee socially responsible AIS procurement and conformance with the provisions of this standard. Adoption of the standard does not imply conformance with any particular ethically aligned principles or value systems, which vary from community to community and over time. This standard encourages alignment with the IEEE Ethically Aligned Design Principles [B28] but cannot require conformance to these same principles.

NOTE 3—Users of the standard are responsible for being apprised of and referring to appropriate, applicable local organization and legal requirements and criteria as deemed relevant for consideration during their procurement due diligence.

5. Key concepts

5.1 Guiding principles

The principles in the IEEE Global Initiative on Ethically Aligned Design [B28] are the founding principles that informed this standard's guidance and tools. They are augmented by the principles common to fiduciary agents tasked with a higher bar of professional behavior. Some of these listed next are also reflected in organizations that require a higher duty of care such as that of public entities engaged in providing public services or access to public services. In summary, the ten principles are as follows:

- a) Human rights: Verify AIS does not infringe on jurisdictional and internationally recognized human rights so that these rights are protected through precautionary measures.
- b) Well-being: Prioritize AIS, which has been designed to uphold safety and well-being by mitigating ethical risks.
- c) Accountability: Verify that AIS designers and deployers are responsible and accountable for their claims and attestations.
- d) Transparency: Verify AIS is deployed and operated in a transparent manner in ways lay people can understand (a principle highlighting the value brought to people external to the organization). This principle/value is also reflected in the Universal Guidelines for AI [B10], the right to transparency. It states that individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, logic, and techniques that produced the outcome.
- e) Awareness of misuse: Reduce risks in the misuse of AIS by affording the time to learn the facts and characteristics involved in the misuse of AIS (Ada Lovelace Institute [B2]).
- f) Inclusiveness: Include citizens and consumers as stakeholders capable of evaluating their own interests.

- g) Openness: Verify open, transparent, and inclusive administrative processes from end to end during the procurement life cycle (a principle highlighting the value brought to people internal to the organization).
- h) Competency: Commit to building the required competency and capacity by committing sufficient time and resources for adapting practices to support responsible AIS procurement.
- i) Fidelity: Evaluate AIS vendors and solutions with consistent diligence so as to protect the public interest.
- j) Integrity: Document thoroughly all procurement participants, evaluation, criteria, risks, mitigations, and selection considerations to avoid misrepresentation in any way by acts of commission or omission.

5.2 Adoption flexibility

The standard shall be adopted by one or more of the following user groups:

- a) An organization: To establish an environment of responsible procurement processes. An infrastructure of policies, methods, procedures, techniques, tools, and trained personnel shall support these processes. The organization shall then employ this environment to perform and manage its projects and process systems through its procurement life cycle.
- b) A procurement team: To evaluate and select AIS products and services that meet responsible AIS standards.
- c) A buyer and a supplier: To develop AIS contract clauses, terms, and conditions. Via the contract, the processes and activities in this standard should be selected, negotiated, agreed to, and performed. In this mode, this standard is used for guidance in developing AIS contract clauses, terms, and conditions.

5.3 Interdisciplinary procurement teams

IEEE Std 3119 is most effectively applied when a multidisciplinary and interdisciplinary team is involved—assuming the responsibility for the AIS procurement processes and outcomes across organizational functions, departments, and roles (NIST [B62]). A large multidisciplinary procurement team is not a prerequisite to success, but a cross-functional procurement team is optimal (whether that consists of one program person, a procurement person, and a technology expert or any combination therein). Organizations of any size, even one or two relevant team members with a basic knowledge foundation of AIS and data governance, will benefit greatly from the practical guidance and tools in this standard. Through key roles defined for IEEE 3119 procurement teams in 5.5, this standard seeks to align management and administrative activities with responsible procurement that explicitly works to protect the interests of the public and society.

5.4 Stakeholder engagement

Stakeholders in the procurement process should be divided into two main organizational categories, either internal or external. Internal stakeholders and people are directly connected to the organization through some form of contractual obligation or employment inside the same. They have a strong influence within and/or fulfill internal roles in how the organization achieves its objectives. These people include but are not limited to directors, managers, coordinators, analysts, or executives. External stakeholders are diverse and outside the organization, not usually linked or contractually obligated through employment to the organization. However, external stakeholders still have indirect or direct influence and interest in the

organization's activities. External people could be local communities, non-governmental organizations, other governmental organizations, academia, media, trade unions, AIS vendors, developers, and others.

When acquiring AIS, the procurement team shall demonstrate that it has shown due diligence in identifying the interests of external stakeholders who will be affected by the AIS and made information regarding the risks and benefits of the AIS available to affected communities. In common procurement approaches, AIS vendors and deployers bear great influence and responsibility (to include considerations of risks/impacts that result from AIS responses) on the responsible acquisition of AIS through marketing claims and vendor input into the contract and mechanisms of operation (Sanchez-Graells [B75]). IEEE Std 3119 offers a risk assurance approach to explicitly interrogate vendor interests that often represent an imbalance in power between buyers and sellers due to the AIS knowledge asymmetry, especially in the context of buying AIS that serves the public interest.

5.5 Human in the loop

Historically, technology vendors and organizations have sought increased efficiencies derived from automation and AIS computation in order to 'improve' products and services. However, critical decisions have legal, material, or similarly significant effects on an individual, commonly occurring in high-risk domains (see 1.3.6). In this regard, IEEE Std 3119 is especially useful for AIS use cases where AIS functions are aimed at probabilistic judgments for the automation of critical decisions. In these high-risk use cases, humans need to remain "in-the-loop," but they also need to do so in a strategic way to verify the promised value of the AIS is actually achieved. Therefore, the standard's risk-based approach is optimally applied where human or group discernment in high-risk domains has the potential to be replaced by an AIS. While some responsibilities are ceded (see 3.1) to AIS in such cases, careful oversight remains crucial to maintaining the integrity and accountability of decisions.

5.6 Key roles in AIS procurement teams

5.6.1 General

People are the most important drivers of procurement excellence (Hickok [B23], McKinsey & Company [B60]). The roles and responsibilities outlined in 5.6.1 shall be established to verify a well-rounded procurement team is in place to support the acquisition of the AIS. In consideration of staffing scarcity, limited budgets, AIS governance maturity gaps, workloads, and/or time constraints, procurement team roles may be combined so that one person can assume many roles. Further, for large and complex AIS procurement needs, it is equally acceptable for one role to be shared between more than one individual. There are no requirements for independence of roles. In other words, while it is recommended, it is not required to have one unique team member for each role. However, for optimal success, an AIS procurement team leader shall be designated with responsibility and accountability for the implementation of the IEEE 3119 processes (Clause 6 through Clause 11).

Furthermore, nothing in this standard, neither the content nor outcomes, is meant to be understood to require or even suggest the need for a group of specialists whose workflow is separate from the organization's chosen procurement workflow(s). For example, the same people who perform the activities and tasks in this standard should be responsible for other procurement activities. Personnel who conduct the activities and tasks in this standard are expected to collaborate with their co-workers in a cooperative, integrated, and synergistic manner. What is necessary is that team members should get sufficient time to fully engage in the roles to support responsible AIS procurement. Procurement team members shall be present or send a designee for meetings required for the project.

5.6.2 Procurement team roles and responsibilities

5.6.2.1 Executive sponsor

Role: The executive sponsor is a leader in the organization who is responsible and accountable for all or a portion of the strategic outcomes of the organization, which include the procurement outcomes for which the AIS is intended to address.

Responsibilities are as follows:

- a) Support and enable the procurement.
- b) Receives and directs responses to concerns and information from procurement team members or stakeholders about project and procurement decisions.
- c) Communications with other leaders within the organizations regarding social and technical decisions made regarding the AIS and its intended purpose.

5.6.2.2 Procurement manager (and extended resources)

Role: The procurement manager contributes an understanding of procurement processes and practices to facilitate the acquisition of an AIS that has been effectively evaluated for risks and benefits.

Responsibilities are as follows:

- a) Marries risk-based procurement processes with the needs of the procurement team members, stakeholders, and the organization to navigate risk awareness, risk appetite, risk identification, risk mitigation opportunities, risk controls, and risk monitoring.
- b) Evaluates alternatives and trade-offs in the context of the use case and the organization's long-term strategy.
- c) Optimizes technical solutions to support values among a range of stakeholders and system requirements.
- d) Solicits input and support from extended procurement resources (e.g., legal experts, regulatory experts, financial experts) to identify risks, mitigations, and additional departmental requirements.

NOTE—*Procurement manager* is a general job role/title used to encompass all job titles for procurement professionals that directly conduct or facilitate the procurement functions involved in the procurement life cycle (e.g., procurement officer, contract officer, solicitation manager, tender director).

5.6.2.3 Program manager (and cross-functional resources)

Role: The program manager establishes, directs, and supports the orchestration and communication of the organization's need for the AIS, inclusive stakeholder feedback, cross-functional input and support, the AIS requirements, responsible AIS deployment and performance in a way that is understandable and meaningful to the procurement team and all relevant stakeholders.

Responsibilities are as follows:

- a) Needs and requirements
 - 1) Defines the problem by conducting a thorough root-cause analysis.
 - 2) Establishes risk-aware solicitation requirements utilizing input from internal and external stakeholders (see items b and c below) in collaboration with the procurement manager.

- b) Impacted stakeholder feedback
 - 1) Organizes focus groups, expert panels, or other targeted stakeholder outreach processes to gather evidence on the impact of these systems.
 - 2) Applies societal and public interest perspectives to the recommended AIS and shares perceived value conflicts or lived experiences about the same to better understand the potential impact on individuals and communities.
 - 3) Advocates for the reduction of risks to vulnerable stakeholders in the AIS.
- c) Cross-functional input—General
 - 1) Solicits input and support from cross-functional stakeholders to identify inter-and-intra-departmental requirements and establish clear communications.
 - 2) Records decisions and those who are accountable in a consistent and easily retrievable form.
 - 3) Tracks and reports related decisions to adhere to transparent cross-functional needs.
 - 4) Compiles and maintains the use case documentation and shares the relevant records across departments as needed (ISO/IEC/IEEE 26512:2018 [B49]).
- d) Cross-functional input—Technical
 - 1) Solicits technical expert (e.g., data, systems engineer, cyber, or other who would apply the technical specifications of the architecture in AIS) input to
 - i) Verify solutions meet requirements through technical evaluation and risk assessment.
 - ii) Translate business needs into technical criteria, evaluate vendor solutions for compatibility and performance, and assess risks related to system integration and security.
 - iii) Support the technical evaluation process and contribute critical insights (such as solution selection based on technical requirements, enterprise architecture integration, and security controls) to guide procurement decisions.
 - iv) Help monitor and manage the AIS for changes.
 - 2) Identifies and mitigates integration, security, data quality, and data privacy risks, providing insights to optimize system integrity and safeguard organizational interests.
- e) Deployment
 - 1) Leads the application of knowledge of the AIS target market and context of use for the product.
 - 2) Directs the deployment of the AIS post-procurement process and contracting with the procurement support teams.

NOTE—*Program manager* is a general job role/title used to encompass all job titles for program professionals that directly conduct or facilitate achieving the business goals and objectives involved in the procurement life cycle (e.g., project manager, program manager, business leader).

5.7 Procurement team competency

In addition to the individual roles and responsibilities needed to conduct the activities in this standard, there are competencies that should be demonstrated by each individual and the procurement team as a whole. For example, the procurement team should endeavor to understand and confront the novelty in this emerging field by sourcing the most competent and skilled individuals. The standard requires leaders to identify missing skills and competencies in order to proactively resource procurement team members with the needed strengths and capacity, finding the skill sets externally if necessary. It is prudent to select team roles

on the basis of their competence. In this context, competence is the ability to perform a task correctly, efficiently, and consistently to a high quality, under varying conditions, to the organization's satisfaction. Competency should also be attributed to a group or a procurement team when a task is performed by more than one person in view of the multidisciplinary nature, complexity, or scale. A competent person or procurement team requires the following requisite qualities and capabilities:

- a) Procedural and technical domain knowledge: empirical, academic, or a blend of both.
- b) The experience of application (knowing what works) in different contexts and the requisite skills.
- c) The drive/motivation to achieve the goals and strive for improvement or excellence.
- d) Sharing appropriate behaviors, such as teamwork, leadership, and compliance with professional codes.
- e) The ability to adapt to changing circumstances and demands by creating new practical knowledge or skill (know-how).
- f) The ability to perform the requisite tasks efficiently and reduce waste of physical and virtual resources.
- g) The ability to infer what is required by parties and consistently deliver high-quality work to the satisfaction of the end client(s).
- h) The ability to monitor the AIS for significant changes to the platform that could impact the usefulness of the AIS product or service and the vendor contract.

The right blend of these abilities renders a person or group of people (a team) competent in that they achieve the desired outcomes consistently and efficiently, satisfying or exceeding the expectations of the clients over varying circumstances.

6. Problem Definition Process

6.1 Purpose and scope of the process

The purpose of the Problem Definition Process is to characterize the problem, identify the field of potential solutions, clarify whether an AIS will address the problem, assess stakeholder impacts, and determine the organizational risk appetite for the defined use case. To that end, this process shall incorporate input from multiple stakeholders, including but not limited to, input from the public and relevant communities, along with an assessment of jurisdictional laws and regulations in order to thoroughly identify and assess the potential benefits, risks, and requirements of all prospective AIS.

At this stage of PRE-procurement, this process does not focus on preparing the solicitation or evaluating the vendor or any specific solution (yet).

6.2 Outcomes

As a result of the successful implementation of the Problem Definition Process, achievement of the following outcomes shall be demonstrable:

- a) Internal procurement team members and relevant stakeholders describe the problem and external stakeholders provide their external view on the problem.
- b) The range of solution options is identified, including options that involve AIS.

- c) AIS solution options are assessed for potential benefits and risks.
- d) The risk appetite for the procurement is established.

6.3 Activities and tasks

The procurement team shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the Problem Definition Process. This process occurs during the pre-procurement stage prior to issuing a formal solicitation to interested vendors. The process contains various tools (annexes) referenced in the activities that will aid workflows and provide additional guidance on the sequence of mandated activities. These annexes help the team obtain detailed information from internal and external parties that help produce the process outputs and deliverables useful for an adapted solicitation.

The activities and tasks provide the requirements to define the problem and the approach to the solution. Again, this is the stage prior to a formal solicitation where the organization and/or procurement team identifies the problem it is trying to solve and whether AIS is necessary or other solutions are more appropriate. This process identifies multiple stakeholders, including but not limited to internal stakeholders, civic society, and the public, and gathers their feedback on the perceived problem.

NOTE—These activities can benefit from close cooperation with procurement team members that have knowledge of or experience(s) with AIS procurements and AIS vendors in the target domain of interest (if at all possible or in consultation with a technical expert with relevant AI/ADS subject matter expertise).

- a) Define and describe the problem.
 - 1) Identify and engage relevant internal technical and non-technical stakeholders responsible for the procurement.
 - 2) Produce a brief, *preliminary* articulation of the perceived problem with internal stakeholders and key personnel in the organization. Details are provided in Annex B.
 - 3) Identify and engage relevant external public stakeholders and community members for feedback on their experience with the perceived problem. Engage to verify, validate, and substantiate the problem description and data assumptions. (See Annex C.)
 - 4) Refine the problem description based on public feedback and incorporate the information obtained into the Solicitation or other procurement requirements.
 - 5) Synthesize and evaluate all learnings. Organize the information into a cohesive report that identifies key themes and aligns findings across the internal and external stakeholder engagements. This is done to confirm, support, substantiate, and assess the scope of the problem to be solved, including any essential characteristics. (Output A).
- b) Identify and evaluate **all** possible solutions.
 - 1) Use the information from output A as a reference to conducting the following activities:
 - i) Identify and document an analysis of possible solutions.
 - ii) Identify all non-technical solutions: Document and analyze all possible nontechnical solutions in order to identify if the problem can be solved without an AIS solution. Each analysis shall evaluate whether or not the non-technical solutions have the capacity to address all of the essential problem characteristics; if not, then those characteristics shall be rank-ordered and prioritized for further comparative review with other solution options.
 - iii) Identify non-AIS-enabled solutions or other digital solutions.
 - iv) Identify AIS-enabled solution options: Document all possible AIS-enabled solutions, analyzing whether they address the essential problem characteristics. Within each

analysis, if essential characteristics are not addressed, the AIS identified shall be ranked by their effectiveness for further comparative review with other solution options. AIS options should include the following:

- Commercial AI products and services (most AIS in the public sector are currently procured rather than built in-house, McBride [B59]).
 - Commercial configurable/customizable solutions (part of integrated AIS, e.g., Deloitte as vendor of AIS-enabled services such as healthcare eligibility automated decision systems. See Use Case #4). This is different from hybrid developments.
 - EXCLUSION: In-house or custom-developed solutions (DIY/commissioned systems), which are beyond the scope of this standard.
 - EXCLUSION: Hybrid developments of AIS in partnerships, which are beyond the scope of this standard.
- 2) Analyze the pros and cons of the solutions identified previously to create a short list of viable solution options (Output B).
 - 3) Determine, based on the information derived from the above tasks, one of two possible courses of action:
GATING EVENT
 - i) If no AIS is needed, the procurement team shall return to normal procurement processes without the need for further implementation of IEEE Std 3119.
 - ii) If an AIS is needed, continue with item c).
 - c) Research and determine the legal and regulatory context for AIS.
 - 1) Research local, regional, or national legal and regulatory requirements relevant to the specific AIS category and/or AIS use case. (Such as, but not limited to, national, state, and local statutes and legislation, data protection legislation, and relevant sectoral regulations).
 - 2) Document legal and regulatory requirements prior to deciding risk appetite in item e).

NOTE—AIS-related product registrations, conformity assessments, third-party audits, certifications, etc., required by policy should be identified in advance and clearly cited in the solicitation terms and conditions as requirements.
 - d) Conduct solution options impact assessment.
 - 1) Use the guidance in Annex D to prepare for an impact assessment to evaluate the solution options with internal and external feedback (external from the community and/or stakeholders in the public engaged earlier or similar).
 - 2) Select an impact assessment tool. See examples in Table D.1.
 - 3) Conduct the impact assessment using the tool selected.
 - 4) Consider the similar iterative process conducted with step a) problem definition activity. First, the internal organizational process owner(s) defines the problem; then, with the assistance of the procurement team, the public feedback is used to adapt the final problem description and scope the potential need for specific AI solution options. This iterative process is useful for the impact assessment to gain internal and external feedback on the solution options.
 - 5) Organize the results identifying key elements (Clause 6 output) to inform existing procurement requirements for a specific AI use case (Clause 7 input). The entirety of the information obtained in the Clause 6 process is used to confirm, support, substantiate, and assess the scope, benefits, and risks of the AIS requirements developed in Clause 7.
 - e) Decide an acceptable risk appetite for the procurement.

Determine a risk appetite to establish an acceptable level of risk to measure, evaluate, negotiate, and monitor the AIS (see Annex E). Identify the procurement team's risk appetite level (Output D). The risk appetite will be used as a benchmark when evaluating vendors and solutions and to guide the intensity of risk mitigation controls required in the negotiated contracting and monitoring activities.

6.4 Inputs

The following resources constitute a suitable, but not exhaustive, suite of process inputs:

- a) Annex B—Problem Analysis Tool
- b) Annex C—Public Identification and Engagement Guide
- c) Annex D—Impact Assessment and Global Index
- d) Annex E—Risk Appetite Tool

6.5 Outputs

The following work products constitute a suitable, but not exhaustive, suite of the process deliverables:

- a) Well-defined problem description informed by internal and external feedback
- b) Short list of viable solution options (initial requirements)
- c) Impact assessment on solution options based on internal and external perspectives
- d) Organizational risk appetite level

7. Solicitation Preparation Process

7.1 Purpose and scope of the process

The purpose of the Solicitation Preparation Process is to incorporate AIS requirements into the solicitation to confirm that vendors are qualified stewards of the AIS they are proposing. Strategic AIS requirements and questions make solicitation (sometimes known as requests for proposals or tenders) a core element of achieving effective AIS risk mitigation. When solicitations have risk-aware AIS requirements and questions incorporated, vendors are clearer on the expectations to match and possibly exceed the organization's need for responsible AIS products and services.

At this stage of PRE-procurement, this process does not focus on evaluating the vendor or any specific AIS solution.

7.2 Outcomes

As a result of the successful implementation of the Solicitation Preparation Process, achievement of the following outcomes shall be demonstrable:

- a) Vendor AIS organizational governance maturity requirements and questions are incorporated into the solicitation.

- b) AIS technical requirements and questions regarding responsible AIS choices during development are incorporated into the solicitation.
- c) General and specific AIS solicitation terms and conditions are incorporated into the solicitation.

7.3 Activities and tasks

The procurement team shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the Solicitation Preparation Process during a pre-procurement stage. The process contains various tools (annexes) referenced in the activities that will aid workflows within the procurement team. These annexes will help the procurement team obtain detailed information from internal and external parties that help produce the process output and deliverables useful for adapted solicitation.

NOTE 1—Users of the standard are expected to utilize their own solicitation template(s) as required by the organization and any local or regional context. IEEE Std 3119 does not provide a full solicitation template(s). IEEE Std 3119 only provides tools and resources for its users to augment their existing templates, processes, and practices to incorporate new risk-aware AIS elements.

- a) Consider solicitation needs based on outputs from Process 1. (See Annex F.)
- b) Prepare requirements for vendor AIS organizational governance maturity
 - 1) Using Annex G (Vendor governance assessment guide and questions) and the output from Annex E (Risk Appetite Tool) as a reference, prepare acceptance, selection, and/or evaluation criteria by conducting the following activities:
 - i) Identify selection acceptance criteria related to the vendor(s) AIS organizational governance roles and policies.
 - ii) Identify relevant questions for vendors to respond to that will facilitate evaluation of their achievement with the acceptable selection criteria determined using Annex G.
 - 2) Incorporate selection criteria and vendor evaluation questions from above into the solicitation in conjunction with other relevant vendor selection criteria and questions per traditional solicitation practices.
- c) Prepare requirements for AIS technical specifications.
 - 1) Using Annex H (Solution evaluation questions), and the output from Annex E (Risk Appetite Tool) as a reference, prepare acceptance, selection, and/or evaluation criteria by conducting the following activities:
 - i) Identify selection acceptance criteria related to the technical AIS requirements.
 - ii) Identify relevant questions for vendors to respond to that will facilitate the evaluation of their compliance with the AIS requirements determined using Annex H.
 - 2) Incorporate requirements criteria and vendor evaluation questions from above into the solicitation in conjunction with other relevant solution evaluation criteria and questions per traditional solicitation practices.
- d) Prepare AIS solicitation terms and conditions.

Generalizable terms to mitigate AIS risks, regardless of the type of AIS, shall be incorporated into standard solicitation terms and conditions. Risks that are unique to each procurement shall be addressed through the use of a contract addendum referred to as the *Risk Management Schedule*. Conduct the activities below using the relevant annex and process outputs:

- 1) Incorporate general AIS risk mitigation contract language into standard solicitation terms and conditions.

- i) Compare standard contracting terms and conditions with common AIS terms and conditions in Annex I AIS Contract Language Reference Guide. This comparison is designed for procurement teams to align existing/standard contracting templates and documents with this generalizable AIS contract language (in Annex I) that should be included in contracts for AIS.
- ii) Identify and assess gaps, omissions, or other misalignments in traditional/existing contract template language in order to identify which AIS terms and conditions the organization requires to establish a baseline of responsible AIS risk control and management requirements.
- iii) Incorporate AIS-specific terms and conditions identified above into the solicitation in conjunction with other relevant clauses per traditional solicitation practices.

NOTE 2—It is advisable to update all standard internal contracting documents with identified AIS contract language designed to address general AIS risk controls and management requirements to close the risk gaps in existing contract documents.

- 2) Incorporate specific AIS risk mitigations with the Risk Management Schedule addendum.

The objective of this task is to comprehensively identify and document risks and corresponding mitigation tactics (as an addendum to the contract) that are specific to the procurement at hand. An AIS Risk Management Schedule shall be used to track required risk mitigation controls related to each unique use case.

The AIS Risk Management Schedule is designed to be flexible and shall be modified over the life of the contract where relevant. Accounting for several modifications over time given the changing nature of AIS performance parameters and the maturing landscape of laws and regulations. The schedule shall be attached as a blank schedule for post-hoc use during contract negotiations once all risks and mitigation controls are known based on vendor responses. In the case of vendor self-completion, the blank schedule shall be provided to the vendor. Alternatively, the blank schedule shall be pre-populated based on the knowledge and information the procurement team has regarding the known and known-unknown AIS risks.

- i) Using the Risk Management Schedule template provided in Annex J, incorporate relevant risk mitigation control requirements learned throughout the process along with applicable risk mitigation tactics found in Annex K, Annex L, and Annex M:
 - Identify and document all known and known-unknown risks and related mitigation control requirements related to the use case with which the vendor is expected to comply. Be sure to include the following:
 - Risks and mitigation controls related to fairness, bias, equity, privacy, validity, reliability, transparency, explainability, and unique AIS security risks discovered during the activities and task a) problem definition output and task d) impact assessment outputs conducted in Clause 6.
 - Appropriate legal and regulatory compliance requirements discovered during 6.3, task c) legal and regulatory requirements.
 - Key performance indicators (KPIs), metrics, and breach trigger points to measure ongoing AIS performance surveillance over the life of the contract. See Annex K, Annex L, and Annex M for background information on how to establish effective risk mitigation metrics.
 - Attach the updated Risk Management Schedule revised by the procurement team to the solicitation for use during contract discussions and negotiations (if applicable).

NOTE 3—With each new AIS procurement process, it is prudent for the procurement team to revisit and realign standard contracting documents as necessary.

- ii) In a separate file, for internal use only, document the corresponding risk priority level of each risk mitigation control listed in the contract and on the Risk Mitigation Schedule. Together with the procurement team's documented AIS Risk Appetite Tool (Annex E), these documented risk priority levels will support the procurement team's approach to contract negotiation. Higher risk items shall be treated with a higher degree of priority during the negotiation. Lower risk items can be traded off if necessary.

7.4 Inputs

The following resources constitute a suitable, but not exhaustive, suite of process inputs:

- a) Clause 6—Problem Definition Process, impact assessment, risk appetite tool (completed outputs)
- b) Annex F—Solution Requirements Considerations Guide
- c) Annex G—Vendor Governance Assessment Solicitation Questions
- d) Annex H—Solution Evaluation Questions
- e) Annex I—AIS Contract Language Reference Guide
- f) Annex J—Risk Management Schedule Template
- g) Annex K—AIS Risk Management Metrics Guide
- h) Annex L—AI Governance Trigger Points Guide
- i) Annex M—AIS Auditing Overview Guide

7.5 Outputs

The following work products constitute a suitable, but not exhaustive, suite of the process deliverables:

- a) Vendor AIS organizational governance maturity requirements
- b) Vendor AIS organizational governance maturity questions
- c) Solution technical requirements
- d) Solution technical evaluation questions
- e) Solicitation terms and conditions as follows:
 - 1) Contract clauses
 - 2) Risk Management Schedule

8. Vendor Evaluation Process

8.1 Purpose and scope of the process

The purpose of the Vendor Evaluation Process is to identify AIS vendors that possess an adequate maturity of AIS governance roles and policies to responsibly deliver the preferred AIS. The scope of the Vendor Evaluation Process is to evaluate the level of AIS governance maturity each vendor possesses in order to identify the potential AIS governance risk differences between the prospective vendors. The AIS governance maturity status of the preferred vendor will help identify governance risk controls necessary to incorporate into the contract.

This process excludes elements related to the evaluation of the AIS and model specification being procured.

8.2 Outcomes

As a result of the successful implementation of the Vendor Evaluation Process, achievement of the following outcomes shall be demonstrable:

- a) Evidence of the vendors' AIS governance roles and policies are discovered and documented.
- b) The maturity of each vendor's organizational AIS governance status is assessed and scored.
- c) Vendor risk profiles are documented.
- d) Additional risk mitigation controls are identified and documented for Clause 10, Contract Negotiation Process.

8.3 Activities and tasks

The procurement team shall complete the following activities and tasks in accordance with applicable organization policies and procedures with respect to the Vendor Evaluation Process. This process provides guidance for evaluating the AIS governance maturity of each vendor in this clause.

Once vendor(s) solicitation responses are received and reviewed, a scoring approach using the AI Governance Maturity Scoring Guide (Annex N) shall be used to assess and compare the governance maturity of each vendor. Procurement team reviewers shall evaluate the thoroughness and strength of evidence provided for each question. See Annex N for details.

- a) Review vendors' answers, evidence, artifacts, and improvement plans submitted to the solicitation to assess the vendors' organizational AIS governance practices. This activity consists of the following tasks:
 - 1) Refer to Annex N to complete this activity.
 - i) Review answers, evidence, artifacts, and improvement plans provided by vendors regarding the following AIS governance roles:
 - AIS governance titles, positions within the corporate hierarchy, duties and responsibilities per role, and amount of autonomy and decision authority per role.
 - Experience and qualifications of the individuals performing each of the governance roles.
 - ii) Review answers, evidence, artifacts, and improvement plans provided by vendors regarding the following AIS governance policies:
 - Diverse staffing in disciplinary expertise and demographics (class, race, age, ability, gender, education) and the availability of processes that ensure consideration of all relevant concerns
 - Code of AIS Ethics, Principles for AIS Safeguards, and/or Policy on Responsible AIS Innovation, Development, and Deployment (i.e., IEEE Ethically Aligned Design [B28])
 - Responsible procurement and monitoring of AIS supply chain systems
 - Responsible and trustworthy AIS deployment
 - Ethical training for employees and contractors

- Whistleblower protections
- Adverse incident detection and response policy
- iii) Evaluate additional evidence (improvement plans) to understand how the vendor intends to address any identified deficiencies. The vendor shall provide reasonable evidence of future governance practices to establish increased governance maturity within the contract period. These plans shall contain the following:
 - Sufficient explanations of improved and evolved governance practices
 - Reasonable time-bound goals that occur within the contract period (early enough to be considered beneficial to the majority of the performance of the contract)
- b) Assess and determine the maturity of each vendor's organizational AIS governance status. This activity consists of the following tasks:
 - 1) For each vendor, use a separate blank scoring rubric from Annex N to assign ONE numeric score for each response to each question asked in the solicitation.
 - 2) Calculate the full vendor risk score. Instructions for the rubric and an example are provided in Annex N.
- c) Identify vendors with risk profiles beyond the organization's identified risk appetite.
 - 1) Compare vendor scores and answers side-by-side to rank order vendors from low risk to high risk.
 - 2) Identify high-risk vendors based on weaknesses evident within each vendor's scoring on the AIS Governance Rubric.
 - 3) Identify vendors that demonstrate a risk profile beyond which is deemed acceptable for the solution being sought. These vendors shall be eliminated from further consideration if the risk profile exceeds the acceptable standards established by the procuring entity. Proceed with short-listed vendors only that meet the selection criteria.
- d) Identify risk mitigation needs/requirements for contract negotiation and monitoring purposes based on the discovery of vendor's AIS governance responses.
 - 1) Using the Procurement Risk Register (PRR) Template (see Annex O), create a separate Risk Register for each vendor. Use the respective Risk Registers to document identified vendor risks.

NOTE—For ease of organizing the scope of work, use a separate PRR for individual vendors. Each vendor's PRR will be carried over and used again during the Clause 7, Solicitation Preparation Process to capture deficiencies (also known as risks) with the vendor's proposed AIS.
 - 2) Document deficiencies (also known as risks) on the vendor's respective PRR for each vendor remaining in the competition.
 - 3) Using the PRR for each vendor, also document a recommended AIS governance risk mitigation control or plan(s) for each identified risk. Such plans shall be utilized in the AIS procurement Contract Negotiation Process and Contract Monitoring Process if the vendor is ultimately selected to perform the contract.

8.4 Inputs

The following resources constitute a suitable, but not exhaustive, suite of the process inputs:

- a) Annex N—AI Governance Maturity Scoring Guide
- b) Annex O—Procurement Risk Register

- c) Vendors' responses to questions about their current and planned AIS governance roles and policies

8.5 Outputs

The following work products constitute a suitable, but not exhaustive, suite of the process deliverables:

- a) AIS Governance Maturity scores for each vendor.
- b) List of vendors that meet acceptance criteria.
- c) Documentation containing vendor's individual risks and risk mitigation controls/plans for contract negotiation purposes.

9. Solution Evaluation Process

9.1 Purpose and scope of the process

The purpose of the Solution Evaluation Process is to identify the optimal solution among the offerings provided by the vendors. The scope of this process is to evaluate the benefits and risks presented within the offerings proposed by the vendor(s).

This process excludes elements related to negotiating with vendors.

9.2 Outcomes

As a result of the successful implementation of the Solution Evaluation Process, achievement of the following outcomes shall be demonstrable:

- a) Proposed solutions are evaluated for strengths and weaknesses.
- b) Specific risks and mitigation controls for each solution(s) are identified where applicable.
- c) Vendors'/Solutions risk profiles are compared and evaluated against the solicitation requirements and risk appetite for acceptance considerations.

9.3 Activities and tasks

The procurement team shall complete the following activities and tasks in accordance with applicable organization policies and procedures with respect to the Solution Evaluation Process. This process offers procurement teams the opportunity to identify the optimal solution among offerings provided by vendors. IEEE Std 3119 does not provide specific process steps for the final vendor/solution selection process. It is expected that users of this standard have additional requirements (beyond AIS requirements) to consider and will incorporate IEEE 3119 informational outputs (e.g., vendor scores, identified risks, mitigation controls) into their traditional procurement practices in order to make holistic final selection decisions. Teams shall consider the full landscape of their procurement project requirements in concert with the standard's requirements to build the final vendor/solution selection process.

- a) Evaluate each vendor's proposed solution answers, evidence, artifacts, and plans.
 - 1) Evaluate adherence to and fulfillment of functional requirements stated in the solicitation using the solution evaluation guidelines in Annex P.

NOTE—See Annex Q for additional information on evaluating more advanced AIS.

- b) Identify risks and mitigation controls that will be considered during the Contract Negotiation and Contract Monitoring Processes.
 - 1) For each vendor/proposed solution, use the PRR [Output] to document the risks that are evident in the vendor's proposed solution and establish corresponding mitigation controls.
 - 2) Annotate deficiencies within the solution, including any aspects that the vendor(s) solution does not address.
- c) Identify which vendors/solutions have acceptable and unacceptable risk profiles with respect to the organization's risk appetite.
 - 1) Using the combined inputs from the Organizational AI Governance Maturity assessments conducted during the Vendor Evaluation Process and the Solution Evaluation Process, rank the vendor offerings based on the best, most optimal fit to the procurement requirements to the least, suboptimal fit.
 - 2) In consideration of all possible mitigation controls, it is recommended to eliminate vendors/solutions that do not meet the organization's requirements and/or exceed the organization's risk appetite for procurement.
 - 3) For the purpose of conducting Contract Negotiation (Clause 10), identify the vendor(s) that has/have proposed suitable solution(s) that meet the organization's requirements (with or without reasonable risk mitigation controls) and can accommodate the risk appetite.

9.4 Inputs

The following resources constitute a suitable, but not exhaustive, suite of process inputs:

- a) Vendor responses to relevant solicitation questions about their current and planned AIS governance roles and policies
- b) Answers from Annex E, Risk Appetite Tool
- c) Scores from Annex N, AIS Governance Maturity Scoring Guide on the final set of potential vendors that also match the risk appetite level.
- d) Prioritized list of vendors derived from Annex N.
- e) PRRs for each vendor.
- f) Annex P, Solution Evaluation Guidelines.
- g) Annex Q, AIS types and Use Case Evaluation Supplement.

9.5 Outputs

The following work products constitute a suitable, but not exhaustive, suite of the process deliverables:

- a) Updated solicitation, vendor instructions, and vendor questions related to specific organizational needs and requirements as defined in Clause 6. (See Annex J and Annex K.)
- b) Answers from the PRR along with any deficiency documentation for vendors/solutions that failed the Solution Evaluation Process.
- c) Answers from the PRR along with any additional deficiency documentation to be included in Clause 10, Contract Negotiation Process.

10. Contract Negotiation Process

10.1 Purpose and scope of the process

The purpose of the Contract Negotiation Process is to support negotiating (or renegotiating) final AIS terms and conditions with the selected vendor(s) in order to document specific AIS risks associated with the selected vendor(s) and solution(s), establish the basis for AIS risk management during the period of performance, and establish ongoing compliance with all AIS solution requirements. To inform contract negotiations and complement existing negotiation procedures, this process will incorporate input from all prior process stages.

This process covers only new contract formation and does not cover contract management of active or ongoing contracts.

NOTE—This process is NOT meant to provide legal advice, nor is it meant to replace or displace the procurement team's existing contract negotiation protocols. It is expected that users of this standard will incorporate IEEE 3119 informational outputs (e.g., identified risks and mitigation controls) into their traditional contract negotiation practices in order to secure contracts that best align with organizational AIS governance needs and requirements.

10.2 Outcomes

As a result of the successful implementation of the Contract Negotiation Process, the achievement of the following outcomes shall be demonstrable:

- a) AIS risks and risk mitigation controls specific to the selected vendor(s) and solution(s) are updated on the vendor's Risk Mitigation Schedule.
- b) Final general AIS terms and conditions in the contract and the Risk Management Schedule are negotiated and agreed upon.

10.3 Activities and tasks

The procurement team shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the Contract Negotiation Process. This process guides procurement teams in the negotiation of a contract. This process also incorporates outputs from prior processes (such as vendor PRRs) as inputs to the Risk Management Schedule(s).

- a) Update Vendor Risk Management Schedule(s).
 - 1) Using the AIS Risk Management Schedule output from Clause 7 and information from the PRR from each vendor (output from Clause 8 and Clause 9), perform the following actions:
 - i) Document any additional vendor- and solution-specific risks and risk mitigation controls that are not already addressed on the vendor's Risk Management Schedule.
 - ii) See also Annex K, Annex L, and Annex M for background information on how to establish effective KPIs, metrics, evaluation controls, and breach trigger points for effective AIS risk management.
 - iii) Incorporate requirements to jointly establish an AIS Monitoring and Assurance Plan that will support ongoing contract monitoring (see Clause 11 and Annex R AIS Monitoring and Assurance Plan Template).

- 2) Refer to the separate file created during Clause 7, which documents the corresponding risk priority level of each risk mitigation control listed in the contract and on the original Risk Mitigation Schedule attached to the solicitation. Update the internal file with any newly added items from the Risk Mitigation Schedule and then reassess/re-apply priority levels for all items, as necessary. These documented risk priority levels will support the procurement team's approach to contract negotiation. Higher-risk items shall be treated with a higher degree of priority during the negotiation. Lower-risk items can be traded off where necessary.
- b) Negotiate contract terms and conditions with the selected vendor(s).
 - 1) Using information from the Activity and Task Outputs in 10.2 as a reference, conduct the following activities:
 - i) While negotiating with the selected vendor(s), identify and document points of vendor disagreement within general AIS contract terms and conditions and the Risk Management Schedule. (All general AIS contract language incorporated into the solicitation shall be deemed a high-risk priority subject to only limited revisions or omissions.)
 - ii) Together with the selected vendor(s), review the Risk Management Schedule developed in Clause 7, Activity C. Using the internal risk prioritization document developed in Clause 7 and refined in Activity a) 2) above and subject to relevant laws and regulations, the procurement team shall negotiate in good faith with the vendor(s) Risk Management Schedule provisions according to their associated risk priority level during contract negotiation.
 - 2) Determine one of three possible courses of action:

GATING EVENT

 - i) If no disagreements arise during contract negotiations or all disagreements are resolved, incorporate the agreed-upon language, AIS Risk Management Schedule, and the terms for submitting, reviewing, and finalizing an AIS Monitoring and Assurance Plan into a final contract.
 - ii) If contract disagreements remain unresolved after negotiations but other vendors have been identified, return to Clause 7 to evaluate other vendors.
 - iii) If contract disagreements remain unresolved after negotiations and no other vendors have been identified, return to Clause 6 to reevaluate the need for an AIS solution.
 - iv) The procurement team shall continue negotiations after making this determination; multiple rounds of negotiation are acceptable subject to relevant laws and regulations. However, the procurement team shall not view the lack of alternate vendors or solutions as a reason to reduce AIS risk mitigation or monitoring requirements.

10.4 Inputs

The following resources constitute a suitable, but not exhaustive, suite of process inputs:

- a) Clause 6—Completed AIS Impact Assessment
- b) Clause 6—Completed Organizational Risk Appetite
- c) Clause 7—Solicitation with AIS Terms and Conditions
- d) Clause 7—AIS Risk Management Schedule
- e) Clause 7—Risk Mitigation Schedule—documented priorities
- f) Clause 8 and Clause 9—Vendor(s) response(s) to evaluation questions

- g) Clause 8 and Clause 9—Completed PRR
- h) Annex K—AIS Risk Management Metrics Guide
- i) Annex L—AIS Governance Trigger Points Worksheet
- j) Annex M—AIS Auditing Overview Guide

10.5 Outputs

The following work products constitute a suitable, but not exhaustive, suite of the process deliverables:

- a) Finalized general AIS contract clauses, terms, and conditions.
- b) Finalized Risk Management Schedule (if unique mitigation requirements are anticipated) including:
 - 1) One-time deliverables (e.g., updated vendor-responsible AIS training for all vendor employees, submission of vendor AIS policy on disclosure of AIS use in contracted works)
 - 2) Periodic deliverables (e.g., annual audits, annual attestations)
 - 3) Ongoing risk management actions (e.g., KPIs, metrics)
 - 4) Anomalous actions (e.g., breach triggers and response actions, system upgrades)

11. Contract Monitoring Process

11.1 Purpose and scope of the process

The purpose of the Contract Monitoring Process is to establish effective oversight and management of the AI system (AIS) post-procurement. The Contract Monitoring Process includes the deployment of collaboration methods between the vendor(s) and the buyer to monitor the AIS against the contract requirements, to manage change throughout the AIS deployment life cycle, and to respond to events or incidents where the AIS does not align with the contractually agreed criteria.

The Contract Monitoring Process does not include establishing new contractual AIS performance, risk mitigation requirements, or contract modifications.

11.2 Outcomes

As a result of the successful implementation of the Contract Monitoring Process, achievement of the following outcomes shall be demonstrable:

- a) The AIS Monitoring and Assurance plan is established and implemented.
- b) Pre-deployment activities are conducted to help ensure responsible deployment.
- c) Contractual risk mitigation requirements are monitored.
- d) Routine risk mitigation requirements are managed.
- e) Out-of-range AIS performance measurements are managed.
- f) Decommissioning tasks are considered and planned throughout the AIS life cycle.