ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Technical Research Center

Comparative Analysis of Cybersecurity Standards: Governance versus Engineering Orientations

Technical Whitepaper: ISAU-RP-910-2025-TSvsD10S

Task Group #ISAU-TG62-2025
12-19-2025

An ISAUnited.org Published Whitepaper

Institute of Security Architecture United (ISAUnited.org)

Author or Task Group Number:

ISAU-TG62-2025

Publishing Reviewer(s):

ISAUnited Master Fellow Committee

Affiliation: ISAUnited.org

Authored Date:

November 14, 2025

Published Date:

December 19, 2025

Document Registration Number:

ISAU-WP-910-2025-TSvsD10S

Assigned by the Institute Document Management Register

Publication Notice and Disclosure

This publication is an independent work product of the ISAUnited Technical Research Center. It is offered in good faith to improve technical clarity and defensible practice, and it is not intended to disparage, diminish, or cause harm to any organization, institution, standards body, vendor, or individual.

This publication is not affiliated with, sponsored by, endorsed by, or approved by any third party referenced in the text unless explicitly stated. References to third-party standards, organizations, products, services, trademarks, trade names, and document identifiers are for identification and scholarly discussion only and do not imply endorsement, recommendation, certification, validation, or procurement guidance.

Any scoring, indices, comparative positioning, or analytical conclusions reflect ISAUnited-defined criteria and the authors' professional judgment applied to the stated method and cited evidence. They are informational and are not compliance attestations, certification decisions, legal determinations, or measures of institutional merit.

ISAUnited does not accept payment in exchange for publication decisions. Authors disclose funding and competing interests within the publication.

The full Research Publication Notice and Disclosure is available here: https://www.isauresearchcenter.org/isaunited-publication-disclosure

Abstract

This whitepaper evaluates the extent to which widely used ISO/IEC and NIST publications are applied in practice, distinguishing governance-oriented guidance from engineering-oriented technical standards. ISO and NIST remain essential baselines for governance, risk management, and program oversight. Still, they do not consistently define engineering inputs, measurable outputs, or verification and validation expectations that are required to build defensible architectures. Using five measurement criteria, Technical Specificity, Verifiability, Artifact Output, Granularity, and Lifecycle Integration, and a repeatable scoring method, we compute a composite Engineering Orientation Index and map the results to a quadrant with clearly defined X- and Y-axis definitions. The analysis shows a persistent gap between governance baselines and engineering implementation. The Defensible 10 Standards (D10S) are positioned as the engineering layer that operationalizes baseline intent into measurable requirements, technical specifications, and verification and validation evidence for cybersecurity architecture and engineering practice. This is a coexistence model, not a replacement.

Keywords: ISO/IEC, NIST, Defensible 10 Standards, cybersecurity architecture, cybersecurity engineering, governance orientation, engineering orientation, verification and validation, Engineering Orientation Index, Technical Specificity, Lifecycle Integration, quadrant analysis, comparative analysis, policy as code, infrastructure as code, evidence pack, engineering traceability matrix.

Comparative Analysis of Cybersecurity Standards: Governance versus Engineering Orientations

Introduction

Cybersecurity programs have matured around governance and compliance, yet engineers still lack a common technical layer that specifies how secure systems are designed, built, and validated. This paper examines widely used ISO and NIST publications alongside the Defensible 10 Standards to clarify roles rather than to compete. ISO and NIST remain essential baselines for governance, risk, and control intent. The Defensible 10 Standards provide the engineering layer that translates intent into measurable requirements, technical specifications, and verification and validation evidence. Using five measurement criteria and a repeatable scoring method, we compute a composite Engineering Orientation Index and map results to a two-axis quadrant. The objective is to define the boundary between governance baselines and engineering standards so that security outcomes are provable in modern enterprise environments.

Purpose and Scope

Purpose

The purpose of this whitepaper is to demonstrate role clarity rather than competition. ISO and NIST remain essential baseline references for governance and risk management. The Defensible 10 Standards (D10S) fill the engineering layer: standards that define how practitioners design, build, and validate secure architectures with measurable evidence.

Scope

This study evaluates how selected ISO/IEC and NIST publications function in practice across modern enterprise environments. The scope is limited to cybersecurity

management and control documents that are widely adopted as program baselines and assessment references. Sectoral regulations, product manuals, and vendor playbooks are out of scope.

Each publication is assessed against five measurement criteria: Technical Specificity (TS), Verifiability (VR), Artifact Output (AO), Granularity (GR), and Lifecycle Integration (LI)—scored 0–3, combined into a composite Engineering Orientation Index (EOI), and positioned on a quadrant contrasting governance orientation with engineering orientation. The objective is to clarify roles by delineating where governance baselines end and engineering standards begin, thereby producing measurable, testable implementation.

The 5Ws and How

Who
Cybersecurity architects and engineers; platform, cloud, and software engineering teams; CISOs and security leadership; and governance, risk, and compliance professionals and auditors who rely on baseline standards but increasingly require engineering-grade proof of implementation.

What
ISO and NIST provide baseline guidance for governance, risk management, and control expectations. D10S provides engineering standards that define measurable requirements (inputs), technical specifications (outputs), and verification and validation criteria.

When
As cybersecurity programs have matured toward compliance-heavy practices, demand for technical assurance, measurable validation, and defensible design has outpaced what governance baselines alone can provide.

Where
Modern enterprise environments, including hybrid infrastructure, cloud platforms, software systems, and critical industrial contexts, in which security outcomes must be provable.

Why
Governance baselines answer the question of what an organization should manage. Engineering standards answer how systems must be designed and validated. Without the engineering layer, organizations rely on internal interpretation, tool dashboards, and inconsistent implementation outcomes.

How
D10S operationalizes governance intent by defining engineering requirements,

measurable technical specifications, and expectations for verification and validation evidence. This increases repeatability, reduces interpretive variance, and provides defensible evidence of design integrity.

Methodology

Measurement Criteria

To evaluate the role orientation of ISO and NIST publications, we used five measurement criteria. Each criterion is designed to distinguish governance-oriented guidance (program oversight and risk management) from engineering-oriented standards (measurable design inputs, technical outputs, and verification and validation). This analysis is intended to clarify roles, not to replace or diminish baseline standards. [1]–[5]

Scoring Model

Each criterion is scored on a four-level ordinal scale:

- 0 = primarily outcome-based or descriptive, with broad implementation flexibility
- 1 = partially prescriptive, with limited measurable detail
- 2 = mostly prescriptive, with measurable technical elements and repeatable checks
- 3 = explicitly prescriptive and verifiable, with clear technical requirements and testable outputs

This scoring scale supports inter-reviewer repeatability and reduces subjective interpretation.

Criteria Definitions

1. **Technical Specificity (TS)**
   TS measures whether a publication provides engineering-level implementation requirements or general outcome statements.

   - Score 0: outcome statements such as “encrypt data in transit.”
   - Score 3: implementation requirements such as “enforce TLS 1.3 with approved cipher suites and certificate validation criteria.”

2. Verifiability (VR)
VR measures whether conformance can be validated using deterministic methods

(e.g., scripts, configuration scans, evidence artifacts) or through qualitative assessment driven by interviews, narrative justification, or policy review.

- Score 0: validation primarily relies on audit interviews or policy attestations
- Score 3: validation can be performed using pass fail testing, configuration inspection, or engineering-grade evidence

3. Artifact Output (AO)
AO measures whether the publication explicitly requires engineering artifacts that demonstrate design and build quality, versus documentation artifacts that demonstrate governance intent.

- Engineering artifacts include architecture diagrams, interface contracts, configuration baselines, and evidence packs.
- Governance artifacts include policies, risk registers, and management statements.

4. Granularity (GR)
GR measures the level at which guidance is expressed and evaluated.

- Score 0: enterprise or organizational scope, broad categories
- Score 3: component, interface, protocol, or configuration level scope

5. Lifecycle Integration (LI)
LI measures whether guidance primarily supports governance lifecycle activities (program management, risk oversight, audit readiness) or engineering lifecycle activities (design, build, test, change control, verification and validation (V&V)).

- Score 0: governance lifecycle emphasis
- Score 3: engineering lifecycle emphasis with explicit build and validation expectations

Composite Engineering Orientation Index

To enable consistent comparison across publications, this study combines the five measurement criteria into a single composite metric, the Engineering Orientation Index (EOI). Each criterion is scored on a 0-3 scale, yielding a maximum total score of 15 across the five criteria. EOI is then normalized to the 0-1 range, with higher values indicating a stronger engineering orientation and greater technical verifiability under this framework.

The 15-point maximum represents a theoretical upper limit for a fully engineered, prescriptive, and verifiable standard under the five criteria. Baseline governance

publications are not expected to approach this ceiling, as they are intentionally designed to be outcome-based and flexible in implementation.

EOI is computed using raw criterion values. Rounding is applied only for display purposes. When a criterion is marked not applicable (NA), EOI is calculated using a rescaled denominator, and NA counts are disclosed.

NOTE: The complete formula, normalization, NA handling, and display rules are provided in Appendix A.

Quadrant Mapping

The quadrant in this paper visualizes standards across two dimensions:

- X-axis: Governance-Orientation to Engineering-Orientation
- Y-axis: Outcome-Based and Descriptive to Prescriptive and Verifiable

For pilot plotting, the X-axis is derived from the overall EOI score to represent the composite engineering orientation across all five criteria. The Y-axis is derived from Technical Specificity (TS) and Verifiability (VR) because these two criteria most directly represent prescriptiveness and testability.

The plotting scale and mapping functions used to translate scores into chart coordinates, including handling of overlapping coordinates, are provided in Appendix A.

Foundational Standards Reviewed

This section reviews widely adopted ISO and NIST publications that have shaped cybersecurity practice for decades. The purpose of this review is not to replace, compete with, or diminish these baseline standards. Instead, it clarifies how they function in practice, primarily as governance and risk management guidance that defines what organizations must manage and demonstrate. Using the five measurement criteria in the Methodology section, we assess where ISO and NIST provide governance strength and where they intentionally leave room for interpretation in implementation. This role clarity establishes the technical gap that the Defensible 10 Standards (D10S) were created to fill: engineering-grade standards that define measurable requirements, technical specifications, and verification and validation outcomes for cybersecurity architecture and engineering practitioners.

Analysis of ISO Standards

This section summarizes the ISO and ISO/IEC publications included in this study. The intent is to clarify how these documents function in practice. ISO standards provide essential baseline requirements and governance guidance, but they are not designed to define engineering inputs, measurable outputs, or explicit verification and validation procedures for cybersecurity architecture implementations. This role distinction supports the purpose of this whitepaper and does not imply replacement of ISO standards. [6][7]

ISO I6: ISO/IEC 27001:2022 — Information Security Management Systems (ISMS)
Publication Year: 2022
Summary: ISO/IEC 27001 specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It is structured as a risk-based governance standard that supports organizational oversight and management control. [6]
Measurement Profile: TS: Low; VR: Audit-based; AO: Policy and governance artifacts; GR: Enterprise scope; LI: Management lifecycle
Interpretation: High governance orientation; outcome-based and descriptive.

ISO I1: ISO/IEC 27002:2022 — Information Security Controls
Publication Year: 2022
Summary: ISO/IEC 27002 provides a catalogue of information security controls intended to support risk-based selection and organizational implementation. It offers more control guidance than ISO/IEC 27001, but the statements are generally advisory and allow broad interpretation rather than prescribing testable engineering requirements. [7]
Measurement Profile: TS: Low to Medium; VR: Qualitative assessment; AO: Policy and process artifacts; GR: General control scope; LI: Management and operations
Interpretation: Governance-oriented with partial technical guidance.

ISO I2: ISO IEC 27017:2015 — Security Controls for Cloud Services
Publication Year: 2015
Summary: ISO IEC 27017 extends ISO IEC 27002 with cloud-specific control guidance and shared responsibility considerations for cloud services. It improves clarity for cloud contexts, but it remains control guidance rather than an engineering standard that defines measurable technical outputs and explicit verification and validation procedures. [8]
Measurement Profile: TS: Medium; VR: Audit driven; AO: Guidelines and control interpretation artifacts; GR: Cloud service scope; LI: Operations and governance
Interpretation: Governance-oriented with increased cloud specificity.

ISO I3: ISO IEC 27018:2019 — Protection of PII in Public Clouds
Publication Year: 2019
Summary: ISO/IEC 27018 provides guidance on protecting personally identifiable information in public cloud environments. It strengthens expectations of privacy and cloud privacy governance. Still, it is not structured as an engineering standard, with defined system inputs, measurable outputs, and verification and validation tests for the architecture's implementation. [9]
Measurement Profile: TS: Medium; VR: Audit driven; AO: Guidelines and privacy governance artifacts; GR: Cloud service scope; LI: Operations and governance
Interpretation: Governance-oriented privacy guidance with increased cloud relevance.

ISO I4: ISO IEC 27005 — Information Security Risk Management
Publication Year: 2022
Summary: ISO/IEC 27005 guides information security risk management to support an ISMS. It emphasizes risk identification, analysis, evaluation, and treatment planning. It is designed for governance and risk decision-making, rather than for technical architecture engineering specifications, with measurable build outputs and verification and validation criteria. [10]
Measurement Profile: TS: Low; VR: Audit and governance assessment; AO: risk registers and risk treatment artifacts; GR: organizational and program scope; LI: management and risk lifecycle
Interpretation: Governance-oriented risk standard; descriptive by design.

ISO I5: ISO IEC 27701 — Privacy Information Management
Publication Year: 2025 (Edition 2)
Summary: ISO/IEC 27701 extends the ISMS model to a privacy information management system by adding privacy requirements and guidance. It supports privacy governance and audit readiness for privacy programs. It does not operate as an engineering standard that prescribes technical inputs, measurable outputs, and verification and validation tests for cybersecurity architecture implementations. [11]
Measurement Profile: TS: Low to Medium; VR: Audit driven; AO: privacy management system artifacts and control mappings; GR: organizational scope; LI: management and operations
Interpretation: Governance-oriented privacy standard with control guidance.

Analysis of NIST Standards

This subsection summarizes selected NIST publications commonly used across cybersecurity programs and regulated environments. NIST materials are widely adopted for governance, risk management, and control alignment. Several documents also provide technical guidance, but they generally do not function as engineering standards with defined inputs, measurable outputs, and explicit verification and validation criteria, as D10S is structured.

NIST N7: NIST Cybersecurity Framework (CSF) 2.0
Publication Year: 2024
Summary: NIST CSF 2.0 is a high-level framework that organizes cybersecurity outcomes across six functions: Govern, Identify, Protect, Detect, Respond, and Recover. It is intentionally non-prescriptive to support broad applicability across sectors, organizations, and maturity levels. [12]
Measurement Profile: TS: Low; VR: Qualitative assessment; AO: profiles and tiers; GR: organizational; LI: strategic governance
Interpretation: Governance-oriented; outcome-based and descriptive.

NIST N4: NIST SP 800 53 Rev. 5 — Security and Privacy Controls for Information Systems and Organizations
Publication Year: 2020
Summary: NIST SP 800 53 provides a comprehensive control catalogue used widely across federal and regulated environments. Many controls support technical implementation but are often parameterized, allowing the implementing organization to define key values such as frequency, thresholds, or scope. This enhances flexibility for governance programs, but it also requires engineering teams to translate objectives into specific technical configurations and validation criteria. [13]
Measurement Profile: TS: Medium, often parameterized; VR: mixed audit and testing; AO: system security plan and control implementation evidence; GR: system level; LI: management and operations
Interpretation: Governance-oriented with higher technical detail; not an engineering specification standard.

NIST N2: NIST SP 800 160 Vol. 1 Rev. 1 — Systems Security Engineering: Considerations for a Multidisciplinary Approach
Publication Year: 2022
Summary: NIST SP 800 160 Vol. 1 establishes a systems security engineering approach for building trustworthy systems. It is essential because it formalizes engineering thinking, including requirements analysis, design reviews, and lifecycle integration. However, it does not prescribe technology-specific build requirements, configuration outputs, or test criteria for particular architectures. It serves as a

reference for engineering processes, not a technical standard for implementation. [14]
Measurement Profile: TS: Medium at the process level; VR: process verification; AO: design and engineering documentation; GR: lifecycle; LI: engineering process
Interpretation: Engineering process guidance; descriptive rather than prescriptive technical specification.

NIST N1: NIST SP 800 190 — Application Container Security Guide
Publication Year: 2017
Summary: NIST SP 800 190 provides technical guidance for container security, including common risks in images, registries, orchestration, and runtime environments. This is one of the most technical NIST publications for typical enterprise use. It remains a guide rather than a conformance standard with mandatory engineering requirements, pass/fail criteria, and defined verification and validation outputs. [15]
Measurement Profile: TS: High relative to other guidance; VR: testable in parts; AO: configuration and architecture artifacts; GR: component level; LI: implementation guidance
Interpretation: Technical guidance; not a full engineering standard.

NIST N5: NIST SP 800-171 — Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Publication Year: 2024 (Revision 3)
Summary: NIST SP 800-171 defines security requirements for protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations. It is often used as a compliance and contractual baseline in government supply chains. While it contains specific requirements, it is structured primarily as a requirements catalogue for assurance and assessment rather than an engineering standard that specifies technical architectures, measurable outputs, and explicit verification and validation procedures across domains. [16]
Measurement Profile: TS: Medium; VR: Assessment and audit-driven; AO: SSP, POA&M, and implementation evidence; GR: system and organizational requirements; LI: governance and operations
Interpretation: Governance-oriented requirements baseline with technical content, typically used for compliance assurance.

NIST N8: NIST SP 800-37 — Risk Management Framework (RMF) for Information Systems and Organizations
Publication Year: 2018 (Rev. 2)
Summary: NIST SP 800-37 defines the Risk Management Framework lifecycle for system categorization, control selection, implementation, assessment, authorization, and monitoring. RMF is a governance and authorization model that structures risk decisions and accountability. It does not provide engineering design

specifications or technical build instructions. Instead, it governs how organizations manage risk through process. [17]
Measurement Profile: TS: Low; VR: Audit and process verification; AO: authorization packages, SSPs, risk determinations; GR: organizational and system governance; LI: governance lifecycle
Interpretation: Strong governance and risk framework; outcome-based and descriptive by design.

NIST N3: NIST SP 800-207 — Zero Trust Architecture
Publication Year: 2020
Summary: NIST SP 800-207 defines core concepts, logical components, and deployment considerations for Zero Trust Architecture (ZTA). It is a highly influential architecture reference that helps organizations model identity-driven access and trust boundaries. It provides conceptual clarity and architectural patterns but does not specify domain-level engineering requirements, measurable technical outputs, or explicit verification and validation criteria for specific implementations. [18]
Measurement Profile: TS: Medium; VR: Architecture review and partial testability; AO: architecture diagrams and trust boundary documentation; GR: architecture and system design; LI: design guidance
Interpretation: Architecture doctrine and reference model; more technical than governance frameworks, but still descriptive rather than prescriptive engineering standards.

NIST N6: NIST SP 800-161 Rev. 1 — Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
Publication Year: 2024
Summary: NIST SP 800-161 Rev. 1 guides on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain. It integrates cybersecurity supply chain risk management (C-SCRM) into organizational risk management activities. Although it addresses technical considerations and is widely used in regulated environments, it functions primarily as governance and risk guidance rather than as an engineering standard that defines measurable system inputs, technical outputs, and explicit verification and validation criteria. [19]
Measurement Profile: TS: Medium; VR: Assessment and audit-driven; AO: C-SCRM plans, supplier risk artifacts, assurance evidence; GR: organizational and system scope; LI: governance and operations
Interpretation: Governance-oriented risk guidance with technical relevance; not an engineering specification standard.

Analysis of ISAUnited

Defensible 10 Standards (D10S) Rev.1_2025
Publication Year: 2025
Summary: The Defensible 10 Standards (D10S) define engineering-grade security architecture and engineering expectations across ten domains. Each parent standard specifies Requirements (inputs), Technical Specifications (outputs), Core Principles, Security Control mappings, a dedicated Testing & Validation section, and Implementation Guidance and artifact expectations (e.g., Engineering Traceability Matrices and Evidence Packs). The intent is to operationalize governance objectives into measurable, auditable engineering outcomes. [20]
Measurement Profile: TS: High; VR: High; AO: High; GR: Component/interface level; LI: Engineering lifecycle (policy-as-code, CI/CD gates, drift detection).
Interpretation: Engineering-oriented, prescriptive, and verifiable; designed to complement ISO/NIST baselines by defining the “how” (build, configure, test) and the evidence engineers must produce.
Parent-only scoring note: Sub-standards will elevate TS/VR to 3 where parameterized requirements and formal acceptance criteria are published.

Visual Analysis

The Standards Quadrant

Figure 1 illustrates the core role distinction that underpins the Defensible 10 Standards (D10S). It organizes ISO and NIST publications using two practical questions:

1. What is the document primarily used for in cybersecurity practice: governance and oversight, or engineering and system design?
2. How specific and testable is the guidance: broad outcomes, or verifiable engineering requirements?

This figure is not a ranking of quality, and it does not suggest discontinuing ISO or NIST. ISO and NIST remain essential baseline references for governance and risk management. The purpose of the quadrant is to clarify roles: it shows why cybersecurity also requires an engineering standards layer designed for architects and engineers.

Axis Definitions

X-axis: Governance Orientation to Engineering Orientation
The horizontal axis indicates whether a publication is primarily used for governance and risk oversight or for technical design and engineering execution.

Y-axis: Descriptive to Prescriptive and Verifiable
The vertical axis indicates whether a publication is written as outcome-based guidance or as more prescriptive guidance that can be tested and verified in implementation.

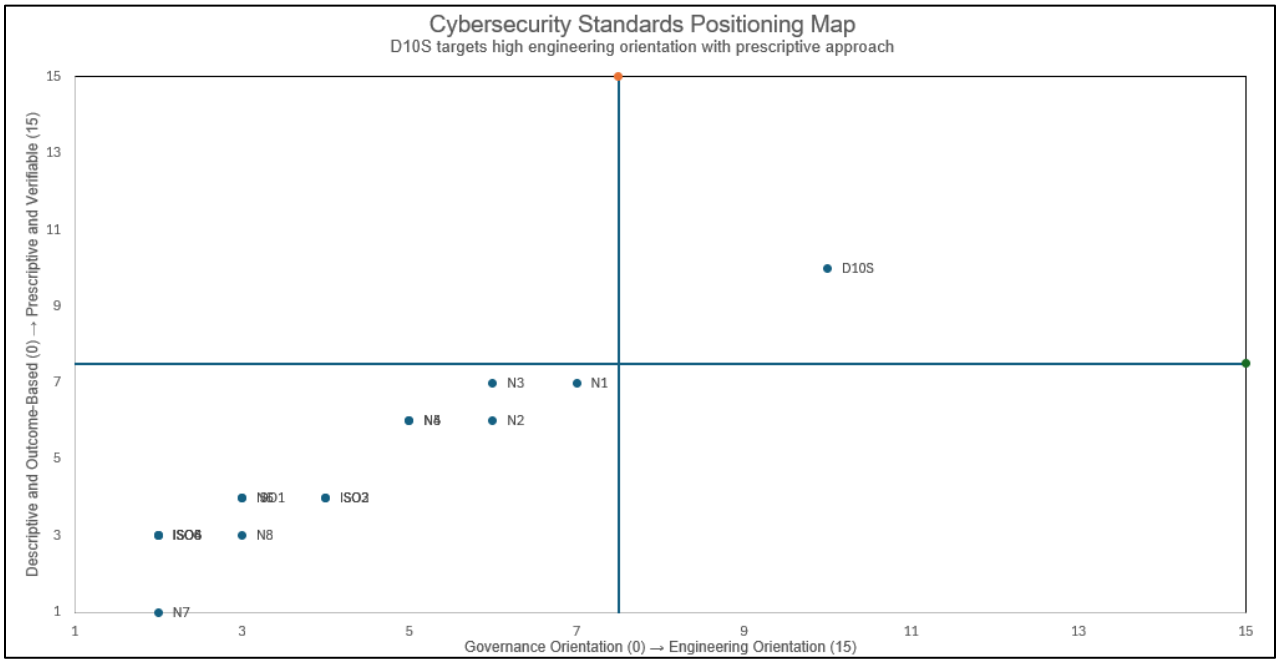
How to read the chart

Publications that cluster toward the governance side are strong for program structure, risk management, and audit alignment. Publications that rise toward the prescriptive and verifiable area provide increasing technical guidance. The D10S is positioned in the engineering and verifiable region because it is designed to define measurable requirements, technical specifications, and verification and validation expectations for defensible cybersecurity architecture.

Reproducibility and scoring

The positions in Figure 1 are derived from the scoring method described in the Methodology. The complete scoring model, mapping rules, and rounding logic are provided in Appendix A. Where multiple publications share the same score and appear to overlap, markers may be slightly offset for readability; the underlying values remain unchanged.

Figure 01. Cybersecurity Standards - Governance vs Engineering Matrix:



Cybersecurity Standards: Governance vs. Engineering Matrix

How to Read the Quadrants

Bottom-Left (Governance and Descriptive).

Documents in this quadrant are strongest for organizing cybersecurity programs, risk management, and audit alignment. They define outcomes and control intents but intentionally leave implementation decisions to the organization. Examples include ISO/IEC 27001 and the NIST Cybersecurity Framework.

Center-Left (Governance with Technical Guidance).

Documents here remain governance-oriented but include more detailed control language or technical guidance. For example, NIST SP 800-53 provides a comprehensive control catalog, but many controls require the implementing organization to define parameters, thresholds, and frequencies. ISO/IEC 27002 also includes control guidance, but it is not structured as an engineering specification with defined system inputs, outputs, and verification criteria.

Center (Engineering Process Guidance).

Some publications focus on security engineering practice, including requirements analysis, design reviews, and lifecycle thinking. NIST SP 800-160 is important because it strengthens engineering process maturity, but it does not prescribe technology-specific engineering outputs or pass/fail verification criteria for particular architectures.

Top-Right (Engineering-Oriented, Prescriptive, and Verifiable).

This quadrant represents standards that define measurable requirements, technical specifications, and explicit verification and validation expectations. Within mainstream cybersecurity publications, this space is sparsely populated. The Defensible 10 Standards are positioned here because they are structured to define engineering inputs and outputs and to require verification and validation evidence that architects and engineers can test, measure, and defend.

NOTE: As sub-standards are approved, D10S points will move further toward the upper-right as parameterized requirements and formal acceptance criteria are published.

Quadrant Scoring Results

The quadrant chart in Figure 1 is a visual summary. These tables provide the underlying scoring data used to generate the plotted positions. They are included to ensure transparency and reproducibility for readers who prefer to review the evaluation logic directly rather than rely solely on the visual.

Each publication is scored against the five measurement criteria defined in the Methodology:

- Technical Specificity (TS)
- Verifiability (VR)
- Artifact Output (AO)
- Granularity (GR)
- Lifecycle Integration (LI)

The five criterion scores are summed to yield a Raw Total, which is then normalized to the Engineering Orientation Index (EOI). The EOI and the combined Technical Specificity and Verifiability values are then mapped to the display coordinates used in the quadrant chart.

Important note for readability: the quadrant may show overlapping points because multiple publications share the same or similar scores. The tables eliminate that ambiguity by listing every score explicitly.

The complete scoring formulas, normalization rules, and mapping logic are documented in Appendix A. This section presents the final scored values and the coordinates plotted for the quadrant.

Table 01. ISO Standards Scoring (Quadrant Inputs):

ID	Standard	TS	VR	AO	GR	LI	Raw Total	EOI (0-1)	*X: Eng (1-10)*	*Y: Presc (1-10)*
ISO6	ISO/IEC 27001	0	1	0	0	0	1	0.07	*2*	*3*
ISO4	ISO/IEC 27005	0	1	1	0	0	2	0.13	*2*	*3*
ISO5	ISO/IEC 27701	0	1	1	0	0	2	0.13	*2*	*3*

ID	Standard	TS	VR	AO	GR	LI	Raw Total	EOI (0-1)	*X: Eng (1-10)*	*Y: Presc (1-10)*
ISO1	ISO/IEC 27002	1	1	1	0	1	4	0.27	*3*	*4*
ISO2	ISO/IEC 27017	1	1	1	1	1	5	0.33	*4*	*4*
ISO3	ISO/IEC 27018	1	1	1	1	1	5	0.33	*4*	*4*

Table 02. NIST Standards Scoring (Quadrant Inputs):

ID	Standard	TS	VR	AO	GR	LI	Raw Total	EOI (0-1)	*X: Eng (1-10)*	*Y: Presc (1-10)*
N7	NIST CSF 2.0	0	0	1	0	1	2	0.13	2	1
N8	NIST SP 800-37	0	1	1	0	1	3	0.20	3	3
N6	NIST SP 800-161	1	1	1	0	1	4	0.27	3	4
N5	NIST SP 800-171	1	2	1	1	1	6	0.40	5	6
N4	NIST SP 800-53	1	2	2	1	1	7	0.47	5	6
N2	NIST SP 800-160 Vol.1	2	1	2	1	2	8	0.53	6	6
N3	NIST SP 800-207	2	2	2	2	1	9	0.60	6	7
N1	NIST SP 800-190	2	2	2	2	2	10	0.67	7	7

Table 03. ISAUnited D10S Scoring (Quadrant Inputs):

D10S	Standard	TS	VR	AO	GR	LI	Raw Total	EOI (0-1)	*X: Eng (1-10)*	*Y: Presc (1-10)*
D1	ISAUnited D10S	3	3	3	3	3	15	1.00	*10*	*10*

Conclusion

The Engineering Gap

This analysis highlights a clear, long-standing gap. ISO/IEC standards are anchored in governance and management systems. NIST standards expand depth through control catalogs and process guidance, yet they remain primarily descriptive or parameterized for local definition. What has been missing is a prescriptive, verifiable engineering layer that specifies inputs and outputs, technical configuration requirements, and explicit verification and validation criteria, much as in traditional engineering disciplines.

Coexistence, Not Replacement

This study does not argue against ISO or NIST. Both are essential. ISO/IEC provides the management system and governance baseline; NIST provides outcome frameworks, control catalogs, and process models. Together, they define what must be governed and achieved. The Defensible 10 Standards (D10S) add the missing how: measurable technical specifications, acceptance tests, lifecycle enforcement, and evidence artifacts that architects and engineers can implement, validate, and defend.

Why Both Layers Are Required

- **Clarity of roles:** ISO/NIST sets policy, outcomes, and control intent; D10S translates those into parameterized requirements, tested configurations, and continuous validation.
- **Assurance, not assertion:** Governance evidence is necessary but insufficient. Engineering evidence—tests, thresholds, artifacts, and drift controls—demonstrates that systems are built and performing as intended.
- **Operational efficiency:** Standardized engineering specifications reduce interpretation variance, rework, and audit friction across teams and vendors.

Path Forward

1. **Adopt a dual-track model:** Retain ISO/IEC and NIST as foundational baselines, and institutionalize D10S as the engineering implementation layer.
2. **Map intent to implementation:** Maintain crosswalks from ISO/NIST clauses to D10S requirements, technical specifications, and verification and validation cases.
3. **Embed verification:** Gate releases on D10S acceptance criteria, monitor for drift, and retain evidence packs as audit-ready artifacts.
4. **Iterate with sub-standards:** Use targeted D10S sub-standards to deepen technical specificity where risk and business impact are highest.

Figure 02. Layered Standards Model:

Governance, Engineering, and Proof: ISO and NIST define the baseline expectations. D10S establishes the engineering requirements and verification and validation needed to produce defensible security outcomes.

Cybersecurity must stand alongside traditional engineering; disciplined, measurable, and defensible. ISO and NIST remain indispensable. D10S completes the picture by providing the engineering standards that turn governance intent into tested, trustworthy systems. Together, these layers establish a coherent, end-to-end standards ecosystem for a safer, resilient, and professionally accountable cybersecurity practice.

Glossary

Crosswalk: Mapping from ISO/NIST clauses to D10S requirements, technical specifications, and verification and validation cases to show intent-to-implementation linkage.

Drift (Configuration Drift): Deviation of a running system from its approved baseline configuration; requires detection, investigation, and corrective action.

Engineering Orientation: Focus on designing, building, and validating systems using measurable requirements, technical specifications, and explicit verification and validation.

Engineering Orientation Index (EOI): Composite score summarizing engineering orientation across TS, VR, AO, GR, and LI (see Methodology).

Engineering Traceability Matrix (ETM): Artifact linking requirements to technical specifications, test cases, and evidence, enabling traceable verification and validation.

Evidence Pack (EP): Collected artifacts (configuration exports, logs, test outputs, and reports) that demonstrate conformance to technical specifications and verification and validation expectations.

Foundational Standards: ISO and NIST publications used for governance, risk management, and control expectations (the what).

Governance Orientation: Focuses on program organization, risk management, and oversight; emphasizes outcomes and accountability over technical implementation detail.

Policy-as-Code (PaC) / Infrastructure-as-Code (IaC): Machine-enforceable policy and infrastructure definitions used to automate control enforcement, gate changes, and prevent drift through version-controlled workflows.

Prescriptive and Verifiable (Y-axis): The degree to which a document defines testable requirements and measurable pass/fail criteria, derived from Technical Specificity (TS) and Verifiability (VR).

Role-Clarity Model (Quadrant): A visualization that distinguishes governance baselines from engineering standards; not a quality ranking.

System-of-Systems (SoS): Interconnected systems (cloud, applications, identity, networks, platforms) that must be secured and verified across components, interfaces, and trust boundaries.

Technical Engineering Standards: D10S documents used for build-level requirements, technical specifications, and verification and validation (the how).

Traditional Engineering: Established engineering disciplines (for example, civil, mechanical, electrical, and systems engineering) that rely on formal standards, measurable specifications, repeatable methods, and verification and validation to design and build safe, reliable systems.

Verification and Validation (V&V): Activities that confirm controls are correctly implemented (verification) and achieve intended outcomes under real operational conditions (validation).

References

[1] International Organization for Standardization, “ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements,” ISO, 2022.

[2] International Organization for Standardization, “ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls,” ISO, 2022.

[3] Joint Task Force Transformation Initiative, “Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5),” NIST, 2020.

[4] R. Ross et al., “Engineering Trustworthy Secure Systems (NIST SP 800-160 Vol. 1 Rev. 1),” NIST, 2022.

[5] M. Souppaya, J. Morello, and K. Scarfone, “Application Container Security Guide (NIST SP 800-190),” NIST, 2017.

[6] ISO/IEC, *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. Geneva, Switzerland: International Organization for Standardization, 2022.

[7] ISO/IEC, *ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Controls*. Geneva, Switzerland: International Organization for Standardization, 2022.

[8] ISO/IEC, *ISO/IEC 27017:2015 Information Technology — Security Techniques — Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services*. Geneva, Switzerland: International Organization for Standardization, 2015.

[9] ISO/IEC, *ISO/IEC 27018:2019 Information Technology — Security Techniques — Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors*. Geneva, Switzerland: International Organization for Standardization, 2019.

[10] ISO/IEC 27005:2022 → (International Organization for Standardization & International Electrotechnical Commission, 2022)

[11] ISO/IEC 27701:2025 → (International Organization for Standardization & International Electrotechnical Commission, 2025)

[12] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD, USA: NIST, 2024.

[13] Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800 53 Revision 5. Gaithersburg, MD, USA: NIST, 2020.

[14] R. J. Ross et al., *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, NIST Special Publication 800 160 Volume 1 Revision 1. Gaithersburg, MD, USA: NIST, 2022.

[15] M. Souppaya, K. Scarfone, and R. Morello, *Application Container Security Guide*, NIST Special Publication 800 190. Gaithersburg, MD, USA: NIST, 2017.

[16] National Institute of Standards and Technology, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171 Revision 3. Gaithersburg, MD, USA: NIST, 2024.

[17] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37 Revision 2. Gaithersburg, MD, USA: NIST, 2018.

[18] National Institute of Standards and Technology, *Zero Trust Architecture*, NIST Special Publication 800-207. Gaithersburg, MD, USA: NIST, 2020.

[19] NIST, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,” NIST Special Publication 800-161 Revision 1, 2024.

[20] ISAUnited.org, “Defensible 10 Standards (D10S): Parent Standards and Sub-Standards,” Defensible10.org, 2025. USA-based, internationally delivered. https://www.defensible10.org. Rev 1, 2025.

Appendix A. Scoring and Quadrant Mapping Equations

A.1 Engineering Orientation Index (EOI)

Each criterion is scored on a 0-3 scale, with a maximum total of 15 across the five criteria.

$$EOI = \frac{TS + VR + AO + GR + LI}{15}$$

Where:
TS = Technical Specificity
VR = Verifiability
AO = Artifact Output
GR = Granularity
LI = Lifecycle Integration
EOI is normalized to the 0-1 range.

A.2 Interpretation of the 15-point maximum

The maximum score of 15 represents the theoretical upper limit for an engineering-grade standard under this framework. Governance baselines are not expected to reach this maximum because they are intentionally outcome-based and implementation-flexible.

A.3 Rounding rules

EOI and component criterion scores are computed using raw values. Rounding is permitted only for display.

A.4 Handling Not Applicable (NA) criteria

If a criterion is marked not applicable (NA), EOI is computed using only the remaining scored criteria using a rescaled denominator, where n is the number of applicable criteria:

$$EOI = \frac{\sum \text{Scored Criteria}}{3 \times n}$$

A.5 Quadrant mapping (0-15 display scale)

The quadrant uses:

- X-axis: Governance Orientation to Engineering Orientation
- Y-axis: Outcome-Based and Descriptive to Prescriptive and Verifiable

For pilot plotting, the mapping produces coordinates directly on a 0-15 chart scale.
X-axis coordinate:

$$X_{15} = 15 \times EOI$$

Y-axis coordinate: TS and VR each range from 0 to 3, so TS + VR ranges from 0 to 6. Normalize to 0-15:

$$Y_{15} = 15 \times \frac{TS + VR}{6}$$

End of Document
IO.