DOI: https://doi.org/10.15276/hait.09.2026.43
UDC 004.056:005.334.1

Risk response compliance framework for organizational information systems: Architecture and sectoral diagnostics

Mark Israel[1)]
ORCID: https://orcid.org/0009-0004-3694-9258; markisr@walla.co.il.
Vyacheslav S. Kharchenko[1)]
ORCID: https://orcid.org/0000-0001-5352-077X; v.kharchenko@csn.khai.edu. Scopus Author ID: 22034616000
[1)] National Aerospace University "Kharkiv Aviation Institute", 17, Vadym Manko St. Kharkiv, 61070, Ukraine

ABSTRACT

Risk Response Compliance – the degree to which an organization's actual information-system risk-response actions match its documented response plans, control requirements and regulatory obligations – remains weakly operationalized as a governance-level indicator, even though it is embedded in established enterprise risk-management practice. **The aim of the article** is to specialize a governance-level Key Performance Indicator framework to Risk Response Compliance and to give it a measurement-ready, self-diagnostic structure. **The research methodology** combines a design-science construction with a measurement model aligned to international information-security measurement standards: seven cross-cutting Risk Response Compliance metrics are defined – Control Implementation Rate, Control Effectiveness Index, Response Plan Adherence Ratio, Audit Defensibility Score, Regulatory Mandate Coverage, Median Time to Compliance and Compliance Stability Index – each normalized to a common dimensionless scale and aggregated by both a linear and a weakest-link (generalized-mean) rule. **The scientific novelty** is a three-directional decomposition of each metric against quality attributes, sectoral compliance constructs and additional dependency families, together with an entropy-based diagnostic index that signals when the metric set must evolve. **The results** are sector-specific weighting profiles derived by expert pairwise comparison, an illustrative numerical example demonstrating the metric algebra, and a boundedness proof for the diagnostic index. **The practical significance** is a conceptual framework that lets organizations measure risk-response compliance jointly as immediacy and defensibility; full empirical validation is defined as future work.

Keywords: Risk response compliance; control effectiveness; ISO/IEC 25010:2023; ISO/IEC 27004; ISO 31000; NIST CSF 2.0; analytic hierarchy process; generalized mean; audit defensibility; Key Performance Indicator framework; framework adaptivity

For citation: **Israel M., Kharchenko V. S. "Risk response compliance framework for organizational information systems: Architecture and sectoral diagnostics". *Herald of Advanced Information Technology.* 2026; Vol.9 No.4: 700–717. DOI: https://doi.org/10.15276/hait.09.2026.43**

INTRODUCTION

Risk Response Compliance (RRC) is one of the most consequential and least operationalized properties of any information system: the degree to which the organization's actual risk-response actions match the response plans documented in its risk-management framework, audit programme, or regulatory mandate. Although the foundational risk management standards ISO 31000 [16] and ISO/IEC 27005 [17] together with the NIST Cybersecurity Framework 2.0 have provided risk-response vocabularies for over a decade, RRC itself remains under-operationalized as a governance-level KPI in the integrated KPI framework of [5]. The 2024-2025 control-effectiveness literature documents that organizations typically implement only a portion of the controls specified in their applicable risk-treatment plans, that the share of controls actually operating in design-effective form is lower still, and that the gap between policy-level commitment and operational compliance is among the largest drivers of audit findings, regulatory penalties, and incident severity [18].

The parent KPI framework [5] maps RRC to a small set of ISO/IEC 25010:2023 attributes: Security, Reliability, Accountability, Effectiveness, and Authenticity. This mapping is necessary but not sufficient. A close reading of the post-2023 RRC literature reveals that compliance is driven by at least four additional families of determinants that fall outside the ISO/IEC 25010:2023 attribute vocabulary. First, control-catalogue and control-mapping architecture: the NIST CSF 2.0 [19], ISO/IEC 27001 Annex A control catalogue, and SOC 2 trust criteria together provide the operational vocabulary of risk response. Second, audit-trail and forensic-evidence architecture: log immutability, evidence-chain preservation, and audit-package automation determine whether a control is provably operational [20], [21]. Third, regulatory-mandate stratification: organizations now operate under a layered set of regulatory mandates (EU AI Act,

© Israel M., Kharchenko V., 2026

This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/deed.uk)

NIS2, GDPR, sector-specific PCI DSS or HIPAA) that impose differentially weighted compliance obligations [22], [23]. Fourth, AI-assisted compliance automation: AI-DSS can act as a compliance-routing layer that automates control-implementation evidence collection and continuously monitors control-effectiveness drift [10], [15], [24].

The earlier IS-quality study by Israel and Kharchenko [14] established a foundational principle that this paper extends. In their analysis of GIS-project quality, the authors argued that the quality of an information system in a specific domain can be modeled as a linear combination of service quality, software quality, and information quality, with weighting determined by domain context [14]. The present paper applies the same compositional logic to RRC: organizational compliance is a convex combination of cross-cutting compliance-behaviour metric values, with sector-specific weighting determined by domain context, as formalized below. The recent companion specialization of [5] to AI Adoption [15] established the cross-KPI interaction between AIA and RRC: AI-DSS simultaneously routes compliance-monitoring and accelerates AIA. The present paper builds on these results by formalizing the four lateral compliance-determinant families.

This paper addresses three interrelated gaps in the literature. First, the canonical risk-management vocabulary of ISO 31000 [16] and ISO/IEC 27005 [17] is process-oriented and lacks measurement-ready governance KPIs at the response-compliance level. Second, the recent practitioner literature on control-effectiveness is rich in case evidence but lacks an integrated dependency model that brings together the five families of determinants identified above into a single framework aligned with the ISO/IEC 25010:2023 attribute vocabulary [1], [5]. Third, the legacy of intelligent-systems quality evaluation [13], [14] has not yet been generalized to organizational compliance measurement.

The contribution of this work is a five-part construction. First, it consolidates the risk-management standards [16], [17], the NIST CSF 2.0 vocabulary [19], the audit-trail literature [20], [21], the regulatory-mandate literature [22], [23], the AI-assisted compliance literature [10], [15], [24], the GIS-quality precedent [14], and the defect-profile tradition [13] into a single integrated RRC architecture. Second, it defines seven new cross-cutting RRC metrics in measurement-ready form. Third, it establishes three parallel dependency mappings: vertical (sectoral), horizontal (ISO per [5]), and lateral (the four additional families). Fourth, it formulates sector-specific weighting profiles consistent with [5] and provides a control-effectiveness interpretation of compliance measurement. Fifth, it provides an explicit Discussion section addressing efficacy, adaptivity, and capability proof.

STATE OF THE RESEARCH

This section reviews the body of work the proposed framework builds on. The review is structured along the five dependency families that drive RRC: risk-management foundations, control catalogue and control mapping, audit-trail and forensic evidence, regulatory mandate stratification, and AI-assisted compliance automation.

Family 1: Risk-management foundations

The foundational risk-management standard ISO 31000 [16] specifies the risk-response options of avoid, reduce, share, and accept; the information-security risk-management standard ISO/IEC 27005 [17] specializes this vocabulary to information-security risk. The COSO ERM framework and the ISO 31000 family together establish the canonical four-stage risk-response process: identify, assess, treat, and monitor [16]. The 2024–2025 risk-management literature [18] documents that the principal gap is operational, not conceptual: organizations document risk-response plans correctly but execute them incompletely.

Family 2: Control catalogue and control mapping

A second body of work documents the control-catalogue architecture that translates risk-response plans into operational controls. NIST CSF 2.0 [19] provides the most widely adopted post-2023 cybersecurity control catalogue, organized into six functions (Govern, Identify, Protect, Detect, Respond, and Recover). ISO/IEC 27001 Annex A provides 93 controls organized into four themes, with each control specifying the response objective. The control-mapping literature [19] documents that mapping a single control to multiple frameworks (NIST CSF 2.0, ISO/IEC 27001 Annex A, SOC 2, PCI DSS, HIPAA) is now standard practice. Naqvi, Kedziora, Zhang, and Oyedeji [4] confirm that ISO/IEC 25010:2023 sub-characteristics – particularly Security and Reliability – are practically measurable at the control level.

Family 3: Audit-trail and forensic-evidence architecture

A third body of work documents that compliance is provable only if the supporting evidence is itself reliable. The audit-trail literature [20] documents that log immutability (write-once-read-many storage, cryptographic seals, blockchain anchoring) is the technical basis of evidence chain preservation. The forensic-evidence literature [21] documents that audit-package automation – the automated assembly of control-implementation evidence into auditor-ready packages – can materially reduce audit findings. The data-quality literature [8] applies the same logic to operational telemetry.

Family 4: Regulatory mandate stratification

A fourth body of work documents the layered regulatory environment under which organizations now operate. The EU AI Act [22] imposes risk-tiered obligations on high-risk AI systems, including IS-embedded AI. The NIS2 Directive [23] imposes essential and important entity obligations on critical-sector organizations. GDPR has imposed data-protection obligations since 2018; sector-specific mandates (PCI DSS for payment, HIPAA for healthcare) impose additional layered obligations. The Diaz, Aiello, and Boldrini Scrum@PA work [11] documents that public-sector organizations carry additional accountability obligations not seen in pure private-sector deployments.

Family 5: AI-assisted compliance automation

A fifth body of work documents the AI-assisted compliance layer. The AI-DSS work of Almutairi [10] explicitly targets compliance-monitoring in agile risk management. The AI-assisted compliance review [24] documents that AI can act as an attention-routing filter that prioritizes high-severity control-effectiveness deviations. The AI-Adoption companion [15] formalizes the cross-KPI link between AI-DSS-driven compliance routing and AIA acceleration.

Time-critical risk-response domains: latency-bounded compliance

A recurring theme across the five determinant families is that risk-response compliance is not only a matter of whether the correct response is executed, but of how quickly it is executed relative to the window in which the risk can cause harm. In most enterprise-IT settings the tolerable response latency is measured in days or weeks; in a growing class of domains, however, that window collapses to minutes, seconds, or less, and a response that is correct but late is functionally non-compliant. Several regulatory mandates now embed such latency bounds explicitly. The EU AI Act [22] requires that high-risk AI systems support real-time human oversight, including the ability to intervene in or halt the system while it is operating; the NIS2 Directive [23] obliges essential and important entities to issue an early incident warning within 24 hours of becoming aware of a significant incident; and the Digital Operational Resilience Act (DORA) [25] imposes comparable major-incident reporting and near-continuous resilience-testing obligations on the financial sector. In each case the mandate itself fixes a response deadline, so that Median Time to Compliance (MTTC) shifts from a supporting indicator to the binding constraint.

The most demanding instances are AI-based autonomous platforms – autonomous vehicles, unmanned aerial systems, algorithmic and high-frequency trading engines, and AI-driven industrial control and robotics – in which the decision loop is closed by software with no human in the immediate path. Here a detected control-effectiveness deviation, such as a miss-calibrated perception model, a drifted risk threshold, or a compromised sensor channel, must trigger a response – rollback, fail-safe, or human hand-off – within the platform's own control cycle, because the interval between anomaly and irreversible physical or financial consequence may be shorter than any manual review. Safety-critical incident response in such autonomous cyber-physical and operational-technology systems therefore depends on continuous, machine-speed control-effectiveness monitoring and automated evidence capture – precisely the AI-assisted compliance-automation layer of Family 5 [10], [15], [24]. For these domains RRC compliance is governed jointly by response-plan adherence (RPAR), control effectiveness (CEI), and, decisively, median time to compliance (MTTC).

Sectoral evidence of risk-response compliance

Healthcare: HIPAA-driven compliance dominates, with audit-defensibility as the primary metric. Finance and banking: Balaskas et al. [7] document that compliance-driven engagement differs across stakeholder groups; PCI DSS, Basel-aligned operational-risk, and sector-specific anti-money-laundering mandates compose the compliance environment. Industry: the Industry-4.0/5.0 review [6] and the industrial data-quality pipeline [8] document that operational-control

evidence is the primary RRC concern. Public sector: Diaz, Aiello, and Boldrini [11] and Bani-Mustafa et al. [12] document the accountability-and-transparency regime of public-sector compliance.

Human-factor and governance moderators

Ali et al. [2] document that top-management support is a strong predictor of compliance success. Akbar et al. [9] show that transformational leadership is associated with ERP-system compliance through change-management mediation. Almutairi [10] confirms that AI-DSS adoption reshapes compliance-attention allocation. These moderators enter the RRC measurement framework as multiplicative scaling on observed metric values.

Risk-management standards anchoring the framework

Two standards anchor the RRC framework: ISO 31000 [16] and ISO/IEC 27005 [17]. ISO 31000 provides the general risk-management process within which RRC operates; ISO/IEC 27005 provides the IS-specific risk-management process and bridges into the ISO/IEC 27001 control catalogue. Together, these two standards anchor RRC in an internationally recognized vocabulary that complements the product-quality vocabulary of [5].

Measurement heritage: intelligent-systems quality and security measurement

Two foundational sources transfer directly to RRC measurement. First, ISO/IEC 25010:2023 [1], [4] provides the product-quality vocabulary. Second, the INAM and the Defect Profile Life Cycle of Gordieiev, Israel, and Kharchenko [13] formalize the logic of predicted-versus-observed divergence and structural update; the same logic is generalized in this paper to compliance anomalies – when observed compliance diverges persistently from predicted compliance, the metric set must evolve.

The international consensus on constructing information-security effectiveness measures is codified in ISO/IEC 27004:2016 [36], which defines the base-measure / derived-measure / indicator hierarchy for monitoring, measurement, analysis and evaluation of an information-security management system. The seven RRC metrics are formulated as ISO/IEC 27004 indicators built on base measures (counts of applicable, implemented and design-effective controls), which anchors them in the accepted KPI/KRI methodology for information security and closes the conceptual gap with the general measurement standard. Recent information-security governance and measurement studies confirm both the managerial relevance of such indicators and the need to formalize them [37], [38]; the present specialization follows the measurement-framework tradition of this journal [39].

Synthesis: seven gaps motivating the framework

First, an operational gap. The canonical risk-management vocabulary of ISO 31000 [16] is process-oriented and lacks measurement-ready governance KPIs at the response-compliance level.

Second, a dependency-aggregation gap. The literature documents at least five distinct families of RRC determinants, but no existing framework brings them together into a single integrated dependency model.

Third, an attribute-mapping gap. While [5] maps RRC to five ISO/IEC 25010:2023 attributes, the literature does not specify how those attributes interact with the four additional dependency families.

Fourth, a control-decomposition gap. The single-scalar treatment of compliance collapses control implementation, control effectiveness, response-plan adherence, audit defensibility, and mandate coverage into a single number.

Fifth, a regulatory-stratification gap. The layered regulatory environment is fast-evolving yet absent from existing governance KPIs.

Sixth, an industry-context gap. General compliance treatments do not account for structurally different accountability regimes in public- and private-sector deployments [3], [11], [12], [14].

Seventh, a measurement-heritage gap. Established traditions in intelligent-systems quality evaluation [1], [4], software defect-profile life-cycle analysis [13], domain-specific IS-quality measurement [14], risk-management [16], [17], and cybersecurity controls [19] have not yet been generalized to organizational risk-response-compliance measurement.

OBJECTIVE AND TASKS

General objective

The overall aim of this study is to specialize the integrated KPI framework of [5] to Risk Response Compliance by formulating an integrated RRC framework that incorporates five distinct families of dependency determinants alongside the five RRC-relevant ISO/IEC 25010:2023 attributes specified in [5].

Five specific tasks operationalize the overall aim.

Task 1: Conceptual systematization, drawing together ISO 31000 [16], ISO/IEC 27005 [17], NIST CSF 2.0 [19], audit-trail and forensic-evidence literature [20], [21], regulatory-mandate literature [22], [23], AI-assisted compliance literature [10], [15], [24], the GIS-quality precedent [14], and defect-profile lifecycle [13].

Task 2: Definition of seven measurement-ready RRC metrics.

Task 3: Three-directional dependency mapping (vertical, horizontal, lateral).

Task 4: Sectoral weighting profiles internally consistent with [5].

Task 5: Three-stage empirical validation plan using PLS-SEM, AHP, and control-effectiveness statistical modelling.

Three-stage empirical validation plan

Stage 1 is expert review via a Delphi panel of 8-12 IS researchers and risk-management practitioners.

Stage 2 is case-based application across two contrasting organizations (one private, one public) with each of the seven RRC metrics calculated from organizational data – control-implementation registers, audit logs, regulatory-filing records, AI-monitoring telemetry – over a three-month observation window.

Stage 3 is a cross-sector survey (target N = 200) and PLS-SEM analysis, complemented by AHP elicitation for sectoral weight vectors and control-effectiveness statistical modelling (e.g., proportion-effective tests with binomial confidence intervals on control samples).

METHODOLOGY

The framework was developed through a 4-stage conceptual design process mirroring [5] and [15]. At Stage 1 (corpus assembly), an academic anchor set was compiled drawing from risk-management foundations, control catalogues, audit-trail and forensic-evidence literature, regulatory-mandate literature, AI-assisted compliance literature, ISO/IEC 25010:2023, ISO 31000 [16], ISO/IEC 27005 [17], NIST CSF 2.0 [19], performance-measurement, sectoral compliance evidence, human-factor moderators, GIS-quality [14], and defect-profile [13] literatures. At Stage 2 (metric definition), each of the seven cross-cutting RRC metrics was defined in measurement-ready form anchored in control-effectiveness statistical reasoning. At Stage 3 (three-directional dependency mapping), three parallel mappings were constructed: vertical (sectoral), horizontal (ISO), and lateral (additional dependency families). At Stage 4 (sectoral differentiation), metric weights were differentiated by sectoral context and checked for internal consistency with the sectoral priority of RRC within the parent KPI framework [5].

The measurement model follows ISO/IEC 27004:2016 [36]: each RRC metric is specified as an indicator derived from explicit base measures, so that the seven metrics are directly auditable. Two design decisions of the revised framework are fixed at this stage. First, because the metrics are measured on heterogeneous scales, every raw metric is mapped to a dimensionless score in [0, 1] before aggregation (defined in the Formal representation below). Second, the sector weight vectors are elicited by the Analytic Hierarchy Process (AHP) [31]: for each sector the seven metrics are pairwise-compared on Saaty's 1-9 scale by domain experts, the principal eigenvector of the reciprocal comparison matrix yields the weights, and a profile is retained only when its consistency ratio CR < 0.10. The weight profiles reported below are therefore expert-derived priors, to be re-estimated empirically by PLS-SEM/AHP [31], [32] in Stage 3 rather than treated as validated constants.

PROPOSED FRAMEWORK

Framework versus model: a conceptual distinction

Following Gregor [28] and the design-science taxonomy of Hevner, March, Park, and Ram [29], a model is a formal representation expressed as a fixed set of variables, parameters, and explicit equations. The ISO 31000 risk-management process [16] and the NIST CSF 2.0 [19] are models in this strict sense. A framework, in contrast, is a higher-order architectural structure that organizes constructs, models, and methods into a single coherent vocabulary. The proposed RRC framework does not replace ISO 31000 or NIST CSF 2.0; it specifies a slot in the Tier-2 cross-cutting metrics layer into which any validated compliance-behavior model can be inserted. The framework includes an explicit self-diagnostic mechanism that triggers metric-set evolution when persistent divergence is detected.

Specialization of the three-tier architecture to RRC

The proposed framework is the RRC specialization of the three-tier KPI architecture defined in [5] (Fig. 1). In the parent framework, Tier 1 contains 25 measurable quality attributes taken from ISO/IEC 25010:2023, Tier 2 contains the seven governance-level metrics, and Tier 3 contains IS-

success outcomes. For RRC specifically, the present paper sub-decomposes the RRC node of Tier 2 into a measurement-ready instrumental layer of seven cross-cutting RRC metrics (the Tier 2a layer), each driven by three distinct families of inputs: (i) the five RRC-relevant ISO/IEC 25010:2023 attributes from [5] (horizontal), (ii) seven sectoral compliance constructs (vertical), and (iii) four additional dependency families (lateral).

Seven new cross-cutting RRC metrics

Control Implementation Rate (CIR) captures the share of applicable controls from the organization's risk-treatment plan that are documented as implemented in their target operating-effectiveness state, observed from control-implementation registers and configuration-management databases. CIR operationalizes the Security and Reliability attributes of RRC in [5] at the control-implementation level.

Control Effectiveness Index (CEI) captures the share of implemented controls that are operating in design-effective form as verified by independent test (control-effectiveness sample testing, penetration testing, and configuration audit). CEI is the operational counterpart of CIR and inherits its statistical interpretation from the control-effectiveness literature [18].

Response Plan Adherence Ratio (RPAR) captures the share of incidents in the measurement window in which the executed response actions matched the documented response plan. RPAR operationalizes the Reliability and Effectiveness attributes of RRC in [5] at the response-execution level.

Audit Defensibility Score (ADS) captures the share of controls for which the supporting evidence package is auditor-complete, observed from automated audit-package assembly tools [20], [21]. ADS operationalizes the Accountability and Authenticity attributes of RRC in [5] at the audit-evidence level.

Regulatory Mandate Coverage (RMC) captures the share of applicable regulatory mandates (GDPR, EU AI Act, and NIS2, sector-specific) for which an explicit control-mapping coverage statement exists. RMC operationalizes the layered regulatory environment as a first-class metric, capturing a determinant structurally absent from the ISO/IEC 25010:2023 vocabulary.

Median Time to Compliance (MTTC) captures the median elapsed time between identification of a non-compliance condition and restoration of compliance. MTTC operationalizes the Effectiveness attribute of RRC in [5] at the remediation-cycle level.

Compliance Stability Index (CSI) captures the inverse coefficient of variation of the six preceding metrics across consecutive measurement periods. CSI inherits its logic from the Defect Profile Life Cycle of [13] and signals whether compliance gains are sustained or transient – a critical concern in regulatory transitions and during major restructurings.

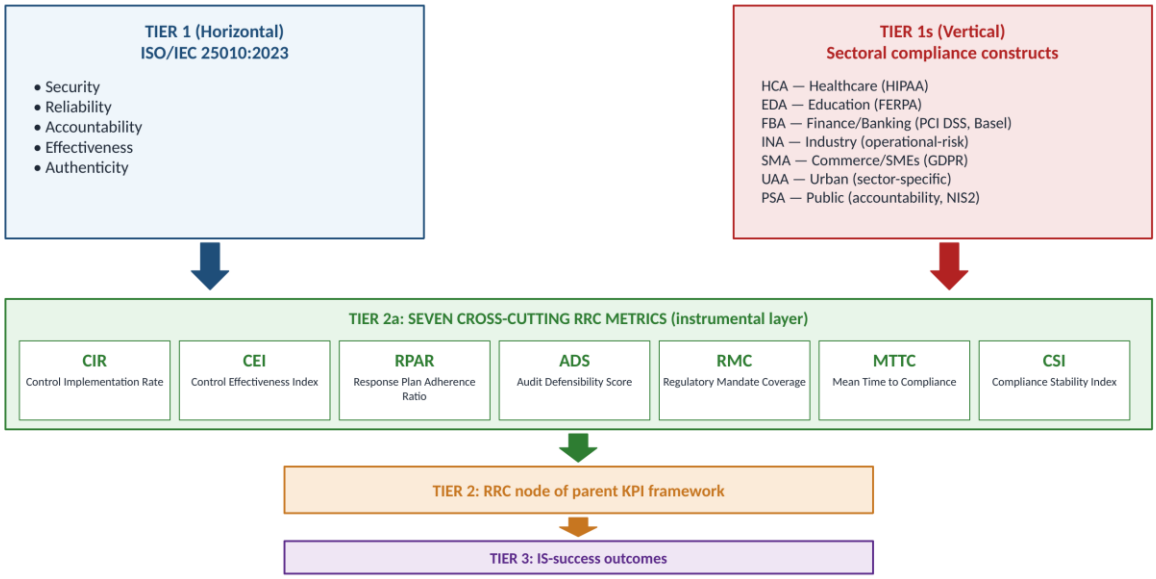


Fig. 1. **The proposed RRC framework as a specialization of the integrated KPI architecture**
Source: **compiled by the authors**

Because the metrics are measured on heterogeneous scales, each is mapped to a dimensionless score before aggregation (see Formal representation): the five proportion metrics are used directly, Median Time to Compliance is mapped by a monotone-decreasing function of the observed median time relative to the sector deadline, and the Compliance Stability Index is mapped through its inverse coefficient of variation rescaled to [0, 1].

Horizontal mapping: RRC metrics × ISO/IEC 25010:2023 attributes

Consistent with [5], RRC is driven by five RRC-relevant ISO/IEC 25010:2023 attributes: Security, Reliability, Accountability, Effectiveness, and Authenticity. The seven cross-cutting RRC metrics inherit this attribute set with the intensities shown in Fig. 2 and Table 1.

Vertical mapping: RRC metrics × sectoral compliance constructs

The seven cross-cutting metrics are linked to seven sectoral compliance constructs through a literature-grounded dependency mapping (Fig. 3; Table 2).

Fig. 3 shows three patterns. First, RRC in finance and banking shows strong linkages with CIR, CEI, ADS, and RMC, reflecting the heavily regulated PCI-DSS and Basel-aligned compliance environment [7]. Second, RRC in industry shows strong linkages with CIR, CEI, RPAR, and MTTC, reflecting the operational-control regime [6], [8]. Third, RRC in the public sector shows strong linkages with ADS, RMC, and CSI, consistent with the accountability- and audit-defensibility-driven regime [3], [11], [12].

Lateral mapping: RRC metrics × four additional dependency families

Four dependency families outside the ISO/IEC 25010:2023 vocabulary are introduced as first-class determinants of RRC: (F1) Control catalogue and control mapping: NIST CSF 2.0 functions, ISO/IEC 27001 Annex A controls, SOC 2 trust criteria [19], [4]; (F2) Audit-trail and forensic-evidence architecture: log immutability, evidence-chain preservation, audit-package automation [20], [21], [8]; (F3) Regulatory-mandate stratification: EU AI Act, NIS2, GDPR, PCI DSS, HIPAA [22], [23]; (F4) AI-assisted compliance automation: AI-DSS-driven control-effectiveness monitoring, automated audit-package assembly [10], [15], [24]. These families and their principal metrics are summarized in Fig. 4 and Table 3.



Fig. 2. **Horizontal dependency mapping of the RRC metrics**
Source: **compiled by the authors**



Fig. 3. **Vertical dependency mapping of the RRC metrics**
Source: **compiled by the authors**

Table 1. **Horizontal mapping of the seven RRC metrics to the five RRC-relevant ISO/IEC 25010:2023 attributes (● strong linkage, ○ secondary linkage)**

Metric	Security	Reliability	Accountability	Effectiveness	Authenticity
CIR	●	●	○	●	○
CEI	●	●	●	●	○
RPAR	○	●	○	●	○
ADS	○	○	●	○	●
RMC	●	○	●	○	●
MTTC	○	●	○	●	○
CSI	○	●	○	●	○

Source: **compiled by the authors**

Table 2. **Vertical mapping of the seven RRC metrics to the seven sectoral compliance constructs (● strong linkage, ○ secondary linkage). Sector codes: HCA Healthcare, EDA Education, FBA Finance/Banking, INA Industry, SMA Commerce/SMEs, UAA Urban, PSA Public**

Metric	HCA	EDA	FBA	INA	SMA	UAA	PSA
CIR	●	○	●	●	●	○	●
CEI	●	○	●	●	○	○	●
RPAR	●	○	●	●	○	○	●
ADS	●	●	●	○	●	○	●
RMC	●	●	●	○	●	○	●
MTTC	○	○	●	●	○	○	○
CSI	○	○	○	●	○	○	●

Source: **compiled by the authors**



Fig. 4. **Lateral dependency mapping of the RRC metrics**
Source: **compiled by the authors**

Table 3. **Lateral dependency families (outside the ISO/IEC 25010:2023 vocabulary) and the principal (●) metric each drives**

Family	Scope / standards	Principal metric
F1 Control catalogue & mapping	NIST CSF 2.0, ISO/IEC 27001 Annex A, SOC 2	CIR, CEI
F2 Audit-trail & forensic evidence	Log immutability, evidence-chain, audit-package automation	ADS
F3 Regulatory-mandate stratification	EU AI Act, NIS2, GDPR, PCI DSS, HIPAA	RMC
F4 AI-assisted compliance automation	AI-DSS effectiveness monitoring, automated evidence	MTTC, CSI

Source: **compiled by the authors**

Sector-specific weighting profiles

In private-sector deployments CIR (0.18), CEI (0.20), and MTTC (0.16) jointly carry the highest weight, with RPAR, ADS, RMC, and CSI as supporting indicators, where control-effectiveness and rapid remediation dominate [6], [7]. In public-sector deployments ADS (0.20), RMC (0.20), and CSI (0.16) carry the highest weight, with CIR (0.14) and RPAR (0.12) as supporting indicators, where audit-defensibility, regulatory coverage, and longitudinal stability dominate [3], [11], [12]. These profiles are internally consistent with the sect

oral prescription for RRC within the parent framework [5]. The resulting profiles are given in Table 4 and visualized in Fig. 5.

The profiles are elicited by AHP pairwise comparison on Saaty's 1-9 scale [31], [40], [41] and accepted only at consistency ratio CR < 0.10; they

are expert-derived priors, not validated constants. A one-at-a-time sensitivity analysis, in which each weight is perturbed by ±20 % and the remainder renormalized, changes the integral RRC of the worked example below by at most ±0.04, so the ordering of sectors by dominant metric is stable under moderate weight uncertainty.

Formal representation: sectoral RRC vectors and weight dynamics

Let $M = \{m_1, m_2, \dots, m_7\}$ denote the ordered set of seven cross-cutting RRC metrics (CIR, CEI, RPAR, ADS, RMC, MTTC, CSI).

For a given sector s, the RRC profile is defined as a non-negative weight vector:

$$w_s = (w_{s,1}, w_{s,2}, \dots, w_{s,7}) \in \mathbb{R}^7,$$
$$w_{s,i} \geq 0, \ \sum_{i=1}^{7} w_{s,i} = 1, \quad (1)$$

where $w_{s,i}$ is the weight of metric i in sector s.

(O1) Addition of a new metric (e.g., a future construct such as an AI-Act-specific compliance index, motivated by [22]):

$$w_s^{'} = \Big((1-\alpha)\, w_{s,1}, \dots, (1-\alpha)\, w_{s,n}, \alpha\Big), \quad (2)$$

where $\alpha \in (0,1)$ is the weight assigned to the newly injected metric under operator (O1).

(O2) Removal of a metric (e.g., MTTC in a deeply manual public-sector deployment with batch remediation cadence [3], [11]):

$$w'_{s,i} = \frac{w_{s,i}}{1-w_{s,k}}, \ \ i \neq k, \quad (3)$$

operator (O2) removes metric k and renormalizes the remaining weights so that they again sum to 1.

Because the seven metrics are measured on heterogeneous scales – five are proportions in [0, 1] (CIR, CEI, RPAR, ADS, RMC), MTTC is a time, and CSI is an inverse coefficient of variation – each raw metric is first mapped to a dimensionless score $v_{s,i}(t) \in [0,1]$–. The five proportion metrics are used directly; MTTC is mapped by $v_{\mathrm{MTTC}} = \min(1,\ T^*/T_{\mathrm{obs}})$, where T^* is the sector deadline and T_{obs} the observed median remediation time, so that $v = 1$ when the deadline is met and $v \to 0$ as it is exceeded; CSI is mapped through its inverse coefficient of variation rescaled to [0, 1]. All aggregation below is defined over the normalized scores $v_{s,i}(t) \in [0,1]$, which makes the weighted combination dimensionally consistent.

(O3) Update of a metric value:

$$\mathrm{RRC}_s^{\mathrm{lin}}(t) = \sum_{i=1}^{7} w_{s,i}\ v_{s,i}(t), \ \ v_{s,i}(t) \in [0,1], \quad (4)$$

linear (convex-combination) aggregation of the normalized metric values.

A purely additive rule cannot represent the weakest-link (bottleneck) behaviour of security controls, in which a design-ineffective control set nullifies a high implementation rate.

The framework therefore also provides a non-linear aggregator – the weighted generalized (power) mean:

$$\mathrm{RRC}_s^{(r)}(t) = \Big(\sum_{i=1}^{7} w_{s,i}\ v_{s,i}(t)^{\,r}\Big)^{1/r}, \ \ r \leq 1, \quad (5)$$

where r is a criticality (hardness) parameter. Equation (5) generalizes (4): $r = 1$ recovers the linear rule; $r \to 0$ gives the weighted geometric (Cobb–Douglas) mean $RRC_s^{(0)} = \prod_i v_{s,i}^{w_{s,i}}$; and $r \to -\infty$ gives the weakest-link operator $\min_i v_{s,i}$. For $r \leq 0$ a critical collapse of any metric (for example $CEI \to 0$) drives $RRC_s^{(r)} \to 0$ even when the remaining metrics are close to 1, so a high control-implementation rate cannot mask an ineffective control set. The parameter r is chosen per sector according to how strongly the weakest-link effect dominates; $r = 1$ is the default baseline.

Human-factor and governance moderators [2], [9], [10] enter multiplicatively on the normalized values:

$$v_{s,i}^{\mathrm{eff}}(t) = \mu_s(t)\, v_{s,i}(t), \quad (6)$$

where $\mu_s(t) \in (0,1]$ is a human-factor / governance moderator (top-management support, audit maturity).

Illustrative numerical example. To demonstrate the metric algebra, consider a hypothetical (anonymized) private-sector deployment with the normalized scores of Table 5 and the private-sector weights of Table 4. The linear rule (4) gives $RRC^{\mathrm{lin}} = 0.71$; the weighted geometric mean
(5, $r = 0$) gives 0.67; and the weakest-link form
(5, $r \to -\infty$) gives $\min_i v_i = 0.35$, set by the low Control Effectiveness Index. The three aggregators agree that overall compliance is dominated by the weakest control dimension: a design-ineffective control set (CEI = 0.35) caps provable compliance regardless of a high implementation rate (CIR = 0.92). This example is illustrative of the equations, not an empirical validation.

Table 4. **Sector-specific weighting profiles w_s (AHP-elicited expert priors; each column sums to 1.00)**

Metric	Private	Public	Hybrid
CIR	0.18	0.14	0.16
CEI	0.20	0.10	0.15
RPAR	0.12	0.12	0.12
ADS	0.10	0.20	0.15
RMC	0.14	0.20	0.17
MTTC	0.16	0.08	0.12
CSI	0.10	0.16	0.13
∑	1.00	1.00	1.00

Source: **compiled by the authors**

Table 5. **Worked example (hypothetical private-sector data): metric weights, normalized values, and contributions to the linear aggregate**

Metric	Weight w_i	Normalized v_i	$w_i \cdot v_i$
CIR	0.18	0.92	0.166
CEI	0.20	0.35	0.070
RPAR	0.12	0.80	0.096
ADS	0.10	0.75	0.075
RMC	0.14	0.88	0.123
MTTC	0.16	0.70	0.112
CSI	0.10	0.65	0.065
RRC^{lin}	1.00	—	0.71

Source: **compiled by the authors**

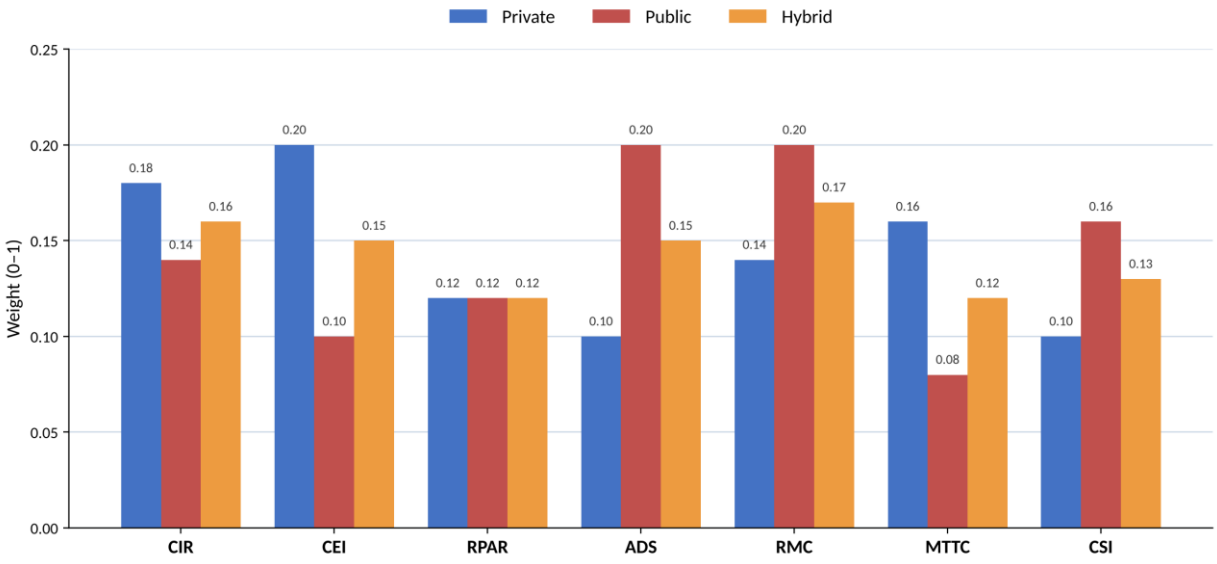


Fig. 5. **Sector-specific weighting profiles for the seven RRC metrics**
Source: **compiled by the authors**

Control-effectiveness interpretation of RRC measurement

RRC differs from the other six governance KPIs of [5] in that its underlying measurements are explicitly statistical: control-effectiveness is verified by sampling, and the resulting estimates carry confidence intervals. The five proportion metrics (CIR, CEI, RPAR, ADS, RMC) are therefore measured by treating each as a population proportion p with sample-based estimator $\hat{p}$ and the Wilson score confidence interval [30]: Fig. 6 summarizes this control-effectiveness interpretation.

$$\frac{\hat{p}+z^2/2n \pm z\sqrt{\hat{p}\,(1-\hat{p})/n+z^2/4n^2}}{1+z^2/n}, \qquad (7)$$

where $\hat{p}$(7) is the sample proportion, n the sample size, and z the standard-normal quantile for the

chosen confidence level. The two non-proportion metrics are estimated by matched interval estimators – MTTC (a time) by a distribution-free interval for the median and CSI (an inverse coefficient of variation) by a bootstrap interval – and are therefore not treated as binomial proportions.

The control-effectiveness view is novel within the RRC literature, which has so far treated compliance as a deterministic count [18].

Diagnostic use of weight vectors: signaling the need for new metrics

Five diagnostic families are proposed. (D1) Concentration and entropy, using the Shannon entropy [35] of the weight vector:

$$0 \le H(w_s) = -\sum_i w_{s,i} \log w_{s,i} \le \log 7 \approx 1.946 \quad (8)$$

(D2) Predictive deficit. (D3) Discriminant-validity failures ($HTMT > 0.85$). (D4) Temporal instability (large $\| \Delta w_s \|_1$). (D5) Predicted-versus-observed weight divergence.

Their combination defines the injection-need index for RRC:

$$\begin{aligned} &\mathrm{INI-RRC}(s) = \lambda_1 \widehat{H}(w_s) + \\ &+\lambda_2 (1 - Q_s^2) + \lambda_3 \widehat{\mathrm{HTMT}}_s + \\ &+\lambda_4 \| \Delta w_s \|_1 + \lambda_5 \delta_s^{(b)}, \end{aligned} \quad (9)$$

where each component is normalized to [0, 1]: $\widehat{H}(w_s) = H(w_s)/\log 7$ is the normalized entropy (Eq. (8)); $Q_s^2 \in [0,1]$ is the Stone–Geisser predictive-relevance statistic [34], so $(1 - Q_s^2)$ is the predictive deficit; $\widehat{HTMT}_s = \min(1, HTMT_s/0.85)$ is the normalized heterotrait–monotrait ratio [33]; $\| \Delta w_s \|_1/2 \in [0,1]$ is the (half) L_1 weight drift between successive periods; and $\delta_s^{(b)} \in [0,1]$ is the normalized predicted-versus-observed divergence. The coefficients satisfy $\lambda_k \ge 0$ and $\sum_{k=1}^{5} \lambda_k = 1$.

$$\begin{aligned} &\text{If } \mathrm{INI-RRC}(s) \ge \theta: \\ &\text{trigger} \frac{\mathrm{O1}}{\mathrm{O2}}; \\ &\text{otherwise apply } (\mathrm{O3})/(\mathrm{O4}), \end{aligned} \quad (10)$$

where $\theta \in [0, 1]$ is a governance-set threshold. Because every component lies in [0, 1] and the λ_k form a convex combination, INI-RRC(s) ∈ [0, 1].

DISCUSSION: EFFICACY, ADAPTIVITY, AND FORMAL PROPERTIES

Efficacy: comparison with prior frameworks

Compared with ISO 31000 [16], the proposed framework retains the process-foundation but adds (i) measurement-ready cross-cutting metrics, (ii) explicit horizontal mapping to ISO/IEC 25010:2023 attributes per [5], (iii) explicit vertical mapping to sectoral constructs, and (iv) explicit lateral mapping to the four additional dependency families. Compared with NIST CSF 2.0 [19], the proposed framework retains the control-function vocabulary but generalizes from cybersecurity-specific to organization-wide IS compliance. Compared with the GIS-quality model of [14], the proposed framework retains the linear-combination principle but generalizes from three components to seven.

Adaptivity: response to evolving evidence

Three layers of adaptivity are built into the algebra. Value-level adaptivity through (O3); weight-level adaptivity through (O4); structural adaptivity through (O1)/(O2). Structural adaptivity is particularly important in the RRC domain because the regulatory environment changes rapidly: each new mandate (e.g., the EU AI Act [22]) is a candidate (O1) injection that creates a new RMC sub-coordinate.

Near-real-time risk response in autonomous AI platforms

The framework's treatment of Median Time to Compliance (MTTC) acquires particular weight in latency-bounded domains. In conventional deployments MTTC is one of seven co-equal metrics; in AI-based autonomous platforms it becomes a gating constraint, because a risk response

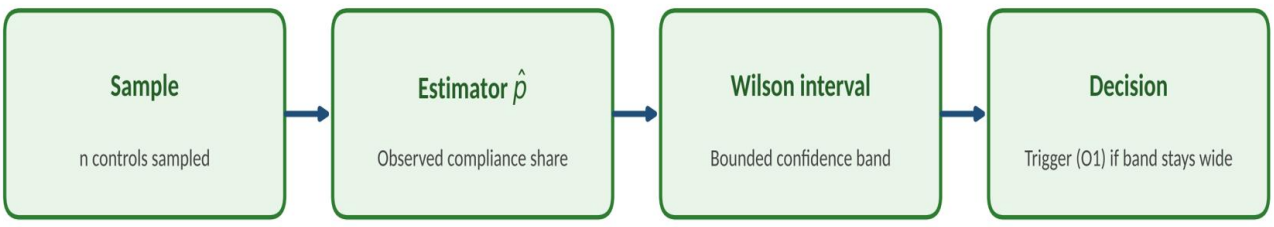


Fig. 6. **Control-effectiveness interpretation of the RRC metrics; the Wilson-score interval is given by Eq. (7)**
Source: **compiled by the authors**

that exceeds the platform's control-cycle deadline fails regardless of how design-effective the underlying control is. The convex-combination form of Eq. (4) accommodates this directly: a sector whose deployments are dominated by autonomous, latency-bounded operation is represented by a weight vector w_s that concentrates mass on MTTC, RPAR, and CEI, in the same way the public-sector profile concentrates mass on ADS, RMC, and CSI. The sector-weighting mechanism of Fig. 5 therefore already expresses the distinction between a response that must merely be correct and one that must be correct and near-immediate, without any change to the underlying algebra.

Two regulatory anchors reinforce this reading. The EU AI Act high-risk regime [22] requires that oversight mechanisms let a human intervene or stop a system in real time, which is a direct constraint on the MTTC of the response actions a compliance framework must document; DORA [25] and NIS2 [23] impose analogous latency-bounded reporting and containment obligations in finance and critical infrastructure. When such a mandate takes effect, it is naturally modelled as an (O1) structural injection (Eq. 2) that adds a latency-specific sub-coordinate – for instance an autonomous-platform response-latency index nested under MTTC – rather than as a mere re-weighting of the existing metrics. This is exactly the structural-adaptivity path that the injection-need index INI-RRC (Eq. 9) is designed to trigger when observed compliance in a latency-bounded domain diverges persistently from predicted compliance.

Autonomous-platform deployments also shift the audit-defensibility burden from periodic evidence assembly toward continuous, tamper-evident telemetry, because the auditable event is no longer a quarterly control test but a machine-speed response that has already executed. Audit Defensibility Score (ADS) and the audit-trail and forensic-evidence family (F2) [20], [21] therefore remain first-class even where MTTC dominates: the response must be both immediate and provable after the fact. This joint requirement – immediacy together with defensibility – is the defining RRC characteristic of AI-based autonomous platforms and motivates their treatment as a distinct latency-bounded weighting profile in future empirical work.

Formal properties of the model

Four properties follow from the algebra. Property 1 (Boundedness): Eq. (1) constrains w_s to the 6-simplex Δ^6. Property 2 (Normalization invariance): operator (O2) preserves $\sum w = 1$ via Eq. (3). Property 3 (Compositional consistency): operator (O1) preserves the simplex via Eq. (2). Property 4 (Diagnostic boundedness): since every component of Eq. (9) is normalized to [0, 1] and the coefficients λ_k form a convex combination ($\sum \lambda_k = 1$), the injection-need index satisfies $\mathrm{INI} - \mathrm{RRC}(s) \in [0,1]$, so the threshold rule (10) is well-defined. These are mathematical properties of the model, not empirical claims.

Limitations

Three limitations: (i) mappings are analytical rather than empirical; (ii) the framework is limited to intra-organizational RRC; (iii) trichotomous sectoral differentiation (private, public, hybrid).

USE CASE: RISK RESPONSE IN AIRBORNE PLATFORMS

Airborne platforms – manned avionics, unmanned aircraft systems (UAS), and emerging autonomous urban-air-mobility vehicles – are the archetypal latency-bounded risk-response domain, and one directly relevant to the aerospace-engineering context of the present work. In flight, the interval between a detected anomaly (a sensor fault, a diverged control law, a mis-classified obstacle) and irreversible physical consequence is measured in seconds or less, so a risk response that is correct but late is indistinguishable from no response at all. The certification basis for airborne software, DO-178C [27], is built on exactly this premise: safety-critical functions must detect and respond to faults – through redundancy switchover, control-law reconfiguration, transition to a safe state, or handoff to a human pilot – within the flight-control cycle rather than within an audit cycle.

The introduction of machine-learning components into airborne platforms sharpens this requirement. The EASA Artificial Intelligence Concept Paper [26] requires that learning-enabled functions be bounded by an explicit operational design domain (ODD) and continuously monitored at runtime, with real-time means for a human to intervene – an aviation-specific instance of the real-time-oversight obligation that the EU AI Act [22] imposes on high-risk AI [26]. The mechanism is concrete: runtime monitoring of ODD parameters safeguards an ML-based perception function during autonomous approach and landing, so that the compliance event is not a quarterly control test but a machine-speed decision that has already executed, and whose correctness must be assured before, not after, the fact.

Cast in the terms of the proposed framework, airborne platforms form a sector whose weight vector w_s concentrates mass on Median Time to Compliance (MTTC), Response Plan Adherence Ratio (RPAR), and Control Effectiveness Index (CEI): the binding question is whether the documented fail-safe response executes within the control-cycle deadline and matches the certified response plan. At the same time, Audit Defensibility Score (ADS) remains first-class, because airborne platforms carry mandatory tamper-evident flight-data and event recording – the response must be both immediate (MTTC) and provable after the fact (ADS), the defining RRC signature of latency-bounded domains. Regulatory Mandate Coverage (RMC) captures the layered aviation mandate stack: DO-178C airworthiness [27], the EASA AI-assurance regime [26], the EU AI Act high-risk regime [22], and NIS2 obligations on critical aviation infrastructure [23].

Because the tolerable response latency of an airborne platform is set by its flight dynamics rather than by an accounting period, this sector is a natural candidate for the structural-adaptivity operator (O1) of the framework: an airborne response-latency index nested under MTTC, triggered by the injection-need index INI-RRC when observed response latency diverges persistently from the certified bound. The airborne use case thus illustrates, in a safety-critical setting, the central claim of this paper — that risk-response compliance must be measured jointly as immediacy and defensibility, and that the sector-weighting and self-diagnostic machinery of the framework accommodates domains where the risk-response window collapses to the duration of a single control cycle.

This use case is presented as an illustrative scenario that exercises the constructs of the framework in a safety-critical setting; it is not an empirical validation of the framework's practical effectiveness.

FUTURE RESEARCH

Beyond the three-stage validation plan, three secondary research lines are anticipated. First, harmonization with the other six governance KPIs of [5] into a single composite IS governance score. Second, integration of EU AI Act, NIS2, and DORA mandate-specific sub-metrics as candidate (O1) injections, drawing on [22], [23]. Third, longitudinal empirical study of the stability of w_s vectors across regulatory transitions (GDPR enforcement, EU AI Act phased entry, NIS2 transposition), which provides a natural quasi-experiment for D4 diagnostics. Besides, in the future, it is advisable to develop a framework for measuring organizational effectiveness that takes into account various project teams [40], [41].

CONCLUSION

Effective assessment of risk-response compliance within an information-systems portfolio requires a measurement architecture in which control implementation, control effectiveness, response-plan adherence, audit defensibility, regulatory mandate coverage, median time to compliance, and longitudinal stability are jointly observable. The seven cross-cutting RRC metrics proposed here (CIR, CEI, RPAR, ADS, RMC, MTTC, CSI) are decomposed in three directions: horizontally, against the RRC-relevant ISO/IEC 25010:2023 attributes specified in [5]; vertically, against sectoral compliance constructs; and laterally, against four additional dependency families (control catalogue, audit-trail and forensic-evidence, regulatory-mandate stratification, AI-assisted compliance automation). The framework's adaptivity, demonstrated through operations (O1)–(O4) and diagnostics (D1)-(D5), is its principal innovation relative to ISO 31000 [16], NIST CSF 2.0 [19], and the GIS-quality model of [14]. Sector context shapes the weight assigned to each metric: private-sector deployments place the highest weight on CIR, CEI, and MTTC; public-sector deployments prioritize ADS, RMC, and CSI. Reliable risk-response compliance remains the ultimate criterion of IS-governed organizational resilience.

As a conceptual framework, its weighting profiles and diagnostic thresholds are expert-derived priors intended for empirical validation (Delphi, case study, and PLS-SEM/AHP) rather than final constants.

DECLARATION ON THE USE OF GENERATIVE AI

In the preparation of this work, the authors used ChatGPT, Claude, and Grammarly for grammar and spelling checks, paraphrasing, and rephrasing. After using these tools, the authors reviewed and edited the content and take full responsibility.

Conflicts of Interest: The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship or other, which could influence the research and its results presented in this article

Financial support: The study was conducted without financial support
Accessibility data: All data are available in digital or graphic form in the main text of the manuscript

Using artificial intelligence tools: During the preparation of this manuscript, the authors used ChatGPT (OpenAI), Claude (Anthropic) and Grammarly for grammatical and stylistic checking, paraphrasing and rephrasing. After using these tools, the authors reviewed and edited the content and take full responsibility for the content of the publication

REFERENCES

1. "Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Product quality model. ISO/IEC 25010:2023". *International Organization for Standardization & International Electrotechnical Commission*. 2023. – Available from: https://www.iso.org/standard/78176.html. – [Accessed: 18 Oct. 2025].

2. Ali, S., Tyagi, A., Gong, Y., Yin, L. & Iqbal, M. "Determinants and outcomes of top management support for information-system projects: A meta-analytic review". *International Journal of Information Management.* 2024; 74: 102702. DOI: https://doi.org/10.1016/j.ijinfomgt.2023.102702.

3. Hertz, H. "2024's CEO challenge: Implement a systems perspective by accelerating the speed of trust". Baldrige Performance Excellence Program. 2024. – Available from: https://www.nist.gov/blogs/blogrige/2024s-ceo-challenge-implement-systems-perspective-accelerating-speed-trust. – [Accessed: 18 Oct. 2025].

4. Naqvi, B., Kedziora, D., Zhang, L. & Oyedeji, S. "Quality of low-code/no-code development platforms through the lens of ISO 25010:2023". *Proceedings of the 29th International Conference on Evaluation and Assessment in Software Engineering (EASE '25 Companion).* 2025. DOI: https://doi.org/10.1145/3727967.3756847.

5. Israel, M. & Kharchenko, V. S. "An integrated KPI framework for organisational information systems: Mapping seven governance-level metrics to ISO/IEC 25010:2023 attributes". *National Aerospace University "KhAI". Working Paper*. 2026; 2: 243–253. DOI: https://doi.org/10.31891/csit-2026-2-20.

6. Bigora, R., Sirisha, S. & Patel, N. "Operationalising organisational performance in the scope of Industry 4.0 and Industry 5.0 in manufacturing companies". *Sustainability*. 2025; 17 (14): 6314. DOI: https://doi.org/10.3390/su17146314.

7. Balaskas, S., Koutroumani, M., Komis, K. & Rigou, M. "Behavioral drivers of AI adoption in banking in a semi-mature digital economy: A TAM and UTAUT-2 analysis of stakeholder perspectives". *Information.* 2025; 16 (2): 137. DOI: https://doi.org/10.3390/info16020137.

8. Costa, D., Almeida, R. & Ribeiro, P. "A data-quality pipeline for industrial environments: Architecture and implementation". *Computers*. 2025; 14 (7): 241. DOI: https://doi.org/10.3390/computers14070241.

9. Akbar, A., Naeem, H., Khan, M. R. & Liu, Y. "Digitalization of present work process: Investigating the role of leadership, change management, and top-management support in the success of enterprise-resource-planning projects". *Sustainability*. 2024; 16 (24): 11178. DOI: https://doi.org/10.3390/su162411178.

10. Almutairi, F. "AI-driven decision-support systems in agile software-project management: Enhancing risk mitigation and resource allocation". *Systems.* 2025; 13 (3): 208. DOI: https://doi.org/10.3390/systems13030208.

11. Diaz, S., Aiello, R. & Boldrini, L. "Scrum@PA: Tailoring an agile methodology to the digital transformation in the public sector". *Information*. 2024; 15 (2): 110. DOI: https://doi.org/10.3390/info15020110.

12. Bani-Mustafa, O., Tucmeanu, R., Tucmeanu, A. I. & Yousaf, Z. "Transforming public-service delivery: A comprehensive review of digitisation initiatives". *Sustainability*. 2024; 16 (7): 2818. DOI: https://doi.org/10.3390/su16072818.

13. Gordieiev, O. O., Israel, M. & Kharchenko, V. S. "Software quality: Injection necessity assessment model and defects profile life cycle". *Information & Security: An International Journal*. 2020; 472. DOI: https://doi.org/10.1007/978-3-031-31488-9_6.

14. Israel, M. & Kharchenko, V. S. "Models for assessing the quality of information systems: analysis and improvement based on GIS projects". *Proceedings of ICTES 2020, CEUR Workshop Proceedings*. Holon, Israel. 2020.

15. Israel, M. & Kharchenko, V. S. “AI adoption across sectors: a comparative review based on the literature and an integrated measurement framework”. *National Aerospace University “KhAI”. Working Paper*. 2026.

16. “Risk management – Guidelines. ISO 31000:2018”. *International Organization for Standardization & International Electrotechnical Commission.* 2018. – Available from: https://www.iso.org/standard/65694.html. – [Accessed: 18 Oct. 2025].

17. “Information security, cybersecurity and privacy protection – Guidance on managing information security risks. ISO/IEC 27005:2022”. *International Organization for Standardization & International Electrotechnical Commission.* 2022. – Available from: https://www.iso.org/standard/80585.html. – [Accessed: 18 Oct. 2025].

18. Giannopoulos, V., Lymperopoulos, A., Kariofyllas, S. & Kariofyllas, C. “Determinants of internal control system effectiveness: Evidence from Greek listed companies”. *Risks*. 2025; 13 (11): 219. DOI: https://doi.org/10.3390/risks13110219.

19. “The NIST Cybersecurity Framework 2.0. NIST CSWP 29”. *National Institute of Standards and Technology*. 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

20. Regueiro, C., Seco, I., Gutiérrez-Agüero, I., Urquizu, B. & Mansell, J. “A blockchain-based audit trail mechanism: Design and implementation”. *Algorithms*. 2021; 14 (12): 341. DOI: https://doi.org/10.3390/a14120341.

21. Nguyen, T. T. B. “Transforming auditing in the AI era: A comprehensive review”. *Information*. 2025; 16 (5): 400. DOI: https://doi.org/10.3390/info16050400.

22. “Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)”. *European Parliament and Council. Official Journal of the European Union*. 2024. – Available from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. – [Accessed: 18 Oct. 2025].

23. “Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)”. *European Parliament and Council. Official Journal of the European Union*. 2022. – Available from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. – [Accessed: 18 Oct. 2025].

24. Duhova, R., Duhov, A., Georgieva, P. & Lazarova, M. “Enhancing enterprise risk management and internal audit practices by applying machine learning models”. *Risks*. 2026; 14 (5): 107. DOI: https://doi.org/10.3390/risks14050107.

25. “Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)”. *European Parliament and Council. Official Journal of the European Union*. 2022. – Available from: https://eur-lex.europa.eu/eli/reg/2022/2554/oj. – [Accessed: 18 Oct. 2025]

26. “Artificial Intelligence Concept Paper Issue 2: Guidance for Level 1 & 2 machine-learning applications”. EASA. 2024. – Available from: https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-concept-paper-issue-2. – [Accessed: 18 Oct. 2025]

27. “DO-178C / ED-12C: Software considerations in airborne systems and equipment certification”. *RTCA, Inc. Washington, DC*. 2011.

28. Gregor, S. “The nature of theory in information systems”. *MIS Quarterly*. 2006; 30 (3): 611–642. DOI: https://doi.org/10.2307/25148742.

29. Hevner, A. R., March, S. T., Park, J. & Ram, S. “Design science in information systems research”. *MIS Quarterly*. 2004; 28 (1): 75–105. DOI: https://doi.org/10.2307/25148625.

30. Wilson, E. B. “Probable inference, the law of succession, and statistical inference”. *Journal of the American Statistical Association*. 1927; 22 (158): 209–212. DOI: https://doi.org/10.1080/01621459.1927.10502953.

31. Saaty, T. L. “Decision making with the analytic hierarchy process”. *International Journal of Services Sciences*. 2008; 1 (1): 83–98. DOI: https://doi.org/10.1504/IJSSCI.2008.017590.

32. Hair, J. F., Hult, G. T. M., Ringle, C. M. & Sarstedt, M. “A primer on partial least squares structural equation modeling (PLS-SEM)”. 3rd ed. Sage, Thousand Oaks. CA, USA. 2022.

33. Henseler, J., Ringle, C. M. & Sarstedt, M. “A new criterion for assessing discriminant validity in variance-based structural equation modeling”. *Journal of the Academy of Marketing Science*. 2015; 43 (1): 115–135. DOI: https://doi.org/10.1007/s11747-014-0403-8.

34. Geisser, S. “The predictive sample reuse method with applications”. *Journal of the American Statistical Association*. 1975; 70 (350): 320–328. DOI: https://doi.org/10.1080/01621459.1975.10479865.

35. Shannon, C. E. “A mathematical theory of communication”. *The Bell System Technical Journal*. 1948; 27 (3): 379–423. DOI: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

36. “Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation. ISO/IEC 27004:2016”. *International Organization for Standardization & International Electrotechnical Commission.* 2016. – Available from: https://www.iso.org/standard/64120.html. – [Accessed: 18 Oct. 2024].

37. Diesch, R., Pfaff, M. & Krcmar, H. “A comprehensive model of information security factors for decision-makers”. *Computers & Security*. 2020; 92: 101747. DOI: https://doi.org/10.1016/j.cose.2020.101747.

38. AlGhamdi, S., Win, K. T. & Vlahu-Gjorgievska, E. “Information security governance challenges and critical success factors: Systematic review”. *Computers & Security*. 2020; 99: 102030. DOI: https://doi.org/10.1016/j.cose.2020.102030.

39. Kotov, I. A., Shvets, D. V., Hryhoriev, Y. I., Karabut, N. O. & Kuttybayev, A. “Applied heuristic information technologies for automating power system management in mining and metallurgical complexes”. *Herald of Advanced Information Technology*. 2026; 9 (2). DOI: https://doi.org/10.15276/hait.09.2026.26.

40. Kononenko, I., Kononenko, O., Babayev, I., Abdullayev, R. “Formalising the formation of project teams considering alternative competence assessments under uncertainty”. *Radioelectronic and Computer Systems*. 2025; 2: 253––263. DOI: https://doi.org/10.32620/reks.2025.2.16.

41. Kononenko, I., Sushko, H., O., Babayev, I., Abdullayev, R. “Solving the problem of ranking applicants for a project team with fuzzy assessment of competencies and requirements”. *Radioelectronic and Computer Systems,* 2024; 2: 230––243. DOI: https://doi.org/10.32620/reks.2024.2.18.

Received 15.08.2026
Received after revision 12.10.2026
Accepted 28.10.2026

DOI: https://doi.org/10.15276/hait.09.2026.43
УДК 004.056:005.334.1

Фреймворк відповідності реагування на ризики в організаційних інформаційних системах: архітектура та галузева діагностика

Ізраель Марк[1)]
ORCID: https://orcid.org/0009-0004-3694-9258; markisr@walla.co.il
Харченко Вячеслав Сергійович[1)]
ORCID: https://orcid.org/0000-0001-5352-077X; v.kharchenko@csn.khai.edu. Scopus Author ID: 22034616000
[1)] Національний аерокосмічний університет «Харківський авіаційний інститут», вул. Вадима Манька, 17 Харків, 61070, Україна

АНОТАЦІЯ

Актуальність. Відповідність реагування на ризики (Risk Response Compliance, RRC) – ступінь, у якому фактичні дії організації з реагування на ризики інформаційних систем відповідають задокументованим планам реагування, контрольним вимогам і регуляторним зобов’язанням – залишається слабко операціоналізованою як показник рівня врядування. **Метою статті** є спеціалізація рамкової системи ключових показників ефективності (KPI) до RRC та надання їй придатної до вимірювання самодіагностичної структури. **Методи** поєднують design-science-побудову з моделлю вимірювання, узгодженою з міжнародними стандартами вимірювання інформаційної безпеки: визначено сім наскрізних метрик RRC (рівень впровадження контролів, індекс ефективності контролів, коефіцієнт дотримання плану реагування, оцінка захищеності аудиту, покриття регуляторних мандатів, медіанний час до відповідності та індекс стабільності відповідності), кожну нормовано до єдиної безрозмірної шкали й агреговано лінійним та слабколанковим (узагальнене середнє) правилами. **Наукова новизна** – трьохнапрямна декомпозиція кожної метрики за атрибутами якості, галузевими конструктами відповідності та додатковими родинами залежностей разом з ентропійним діагностичним індексом, що сигналізує про потребу зміни складу метрик. **Результати** – секторні вагові профілі, отримані експертним попарним порівнянням (AHP),

ілюстративний числовий приклад та доведення обмеженості діагностичного індексу. **Практична значимість** – концептуальний фреймворк для вимірювання відповідності реагування на ризики одночасно як оперативності та доказовості; повну емпіричну валідацію визначено як напрям майбутньої роботи.

Ключові слова: відповідність реагування на ризики; ефективність контролів; ISO/IEC 25010:2023; ISO/IEC 27004; ISO 31000; NIST CSF 2.0; аналітична ієрархія (AHP); узагальнене середнє; захищеність аудиту; система KPI; адаптивність структури

ABOUT THE AUTHORS



Mark Israel - PhD candidate, Department of Cybersecurity and Intelligent Information Technologies. National Aerospace University "Kharkiv Aviation Institute", 17, Vadym Manko Street, Kharkiv, 61070, Ukraine
ORCID: https://orcid.org/0009-0004-3694-9258; markisr@walla.co.il, https://mark-israel.com
Research field: Information-systems quality; governance KPI frameworks; organizational effectiveness measurement

Ізраель Марк - аспірант кафедри Кібербезпеки та інтелектуальних інформаційних технологій. Національний аерокосмічний університет «Харківський авіаційний інститут», вул. Вадима Манька, 17. Харків, 61070, Україна
Галузь досліджень: якість інформаційних систем; системи ключових показників ефективності (KPI) для управління; вимірювання організаційної ефективності



Vyacheslav S. Kharchenko - Corresponding Member of the National Academy of Sciences of Ukraine, Doctor of Engineering Sciences, Professor, Department of Cybersecurity and Intelligent Information Technologies. National Aerospace University "Kharkiv Aviation Institute", 17, Vadym Manko St. Kharkiv, 61070, Ukraine
ORCID: https://orcid.org/0000-0001-5352-077X; v.kharchenko@csn.khai.edu. Scopus Author ID: 22034616000
Research field: Software dependability; AI systems quality; cybersecurity; risk-aware information-systems governance

Харченко Вячеслав Сергійович - член-кореспондент НАН України, д-р техн. наук, професор каф. Кібербезпеки та інтелектуальних інформаційних технологій. Національний аерокосмічний університет «Харківський авіаційний інститут», вул. Вадима Манька, 17.. Харків, 61070, Україна
Галузь досліджень: надійність програмного забезпечення; якість систем штучного інтелекту; кібербезпека; управління інформаційними системами з урахуванням ризиків