Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enterprise Release Assurance for Interconnected Energy Data, Cloud, and Application Platforms A Governance Framework for Coordinated, Multi-Team Release Delivery

Jagadeesh Vedula
IT Project Manager (Digital Transformation)
Meghaz Inc.

ARTICLE INFO

Received: 02 Nov 2023

Revised: 20 Dec 2023

Accepted: 28 Dec 2023

ABSTRACT

While there are times when the production of software or applications are quick and frequent, enterprise-grade software systems are almost never one single development team. The application teams, cloud services, databases, data pipelines, identity platforms, application programming interfaces, security reviewers, infrastructure teams, vendors, business users, and production-support groups are all major stakeholders in a large-scale energy enterprise release. This paper combines the work of release-planning, continuous-delivery, data-quality, cybersecurity, governance-theory, and organizational-culture research to create a model for coordinating releases across interweaving energy data, cloud, and applications platforms: the Enterprise Release Assurance Framework (ERAF). ERAF assesses release readiness in six assurance domains: functional and technical readiness; data integrity and reconciliation; dependency confirmation; cybersecurity and compliance; business and operational readiness; and support, recovery, and stabilization; and combines the evidence in those domains into a composite readiness score that categorizes releases as routine, elevated-risk, or critical. The paper also outlines a common 11-point Release Evidence Package, seven leading risk indicators, and seven outcome-evaluation metrics, such as deployment frequency, change-failure rate and rollback rate. Analysis of releases at each release tier, from each release tier, suggests that differentiating the intensity of the assurance process gives a speedier delivery without the same proportionate amount of operational, security or data-integrity risk. It provides energy companies with a structure that they can use to balance velocity with accountability and reliability in technically interdependent settings.

Index terms: release management; release governance; continuous delivery; data integrity; cybersecurity compliance; cloud computing; dependency management; risk classification; operational readiness; energy information systems; software release planning; organizational culture

I. INTRODUCTION

The increasingly complex and interconnected need for data platforms, cloud infrastructure and end-user-facing applications in the energy sector, co-developed and co-run by many loosely coordinated teams. High frequency delivery practices such as continuous integration and continuous delivery help organizations deliver improvements faster than traditional release cycles do [20], [21].

For critical enterprise environments, a single independent development team is simply not enough—usually a major release relies on application teams, cloud service providers, databases, data pipelines, identity platforms, application programming interfaces (APIs), security reviewers, infrastructure teams, vendors, business users, and production-support groups. This coordination is a recurring governance problem, as it has been observed in decades of research on software release planning [6], [14], [22] without compromising accountability, security and operational reliability.

Energy organizations are dealing with an added layer of difficulty since systems facing upstream, midstream, and downstream operations and energy data intensive systems are required to meet strict cybersecurity and critical infrastructure requirements [5], [7] and reconcile energy data across interdependent pipelines [1], [2].

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

In this paper, the authors present a governance model, the Enterprise Release Assurance Framework (ERAF), that draws on existing release-planning, continuous-delivery, data-quality, cybersecurity, and organisational-culture literature and combines these into one coherent approach applicable to interconnected energy data, cloud, and application platforms. The framework consists of six domains of release assurance, six objective pieces of evidence to determine the composite readiness score, three release tiers: routine, elevated-risk, and critical, and a standardized Release Evidence Package with leading risk indicators and evaluation metrics.

The rest of the paper summarizes the theoretical underpinning to the framework, outlines the six assurance domains, provides a description of the scoring and classification process, and explains how an evaluation can be used and the implications for energy companies looking for faster, safer delivery.

II. BACKGROUND AND RELATED WORK

Since early formulations that characterized software release planning as a combinatorial optimization problem involving balancing feature value, resource constraints and stakeholder priorities [6], [19], software release planning has attracted researchers' attention. There have been many other systematic reviews that identified large numbers of strategic plans to release and emphasized the disconnect between the optimization models that existed in the literature and the judgmental approaches that practitioners employ [3], [22]. Release planning

also exhibits organizational politics, inter-team dependency, and informal negotiation, and these factors are just as important as algorithmic prioritization according to industrial studies [8], [14].

The research moved to focus on continuous integration, delivery and deployment practices as the delivery frequency rose with the adoption of agile and DevOps, with the identification of technical and social barriers that organizations face when attempting to shorten the length of the release cycle, such as test-automation debt, architectural coupling and organizational resistance [4], [12], [20], [21]. The comparative study of release-engineering practice in large and mature organisations versus early-stage startups reveals that requirements for governance grow with the size of the organisations, regulatory exposure and interdependency of systems, but not necessarily with context [13]. A systematic review of agile release-engineering practices also concluded that automation of build, test and deployment tasks enhance release predictability, but also requires sufficient quality-assurance and monitoring practices to not sacrifice reliability for speed of release [9].

Structured, traceable release artifacts have been shown to be synthetically generated directly from the source-control and issue-tracking activity using automated release-note generation research, thus removing the need for manual effort to assemble release documentation [17].

In parallel to the ideas of release engineering, the data-quality literature defines dimensions (e.g., accuracy, completeness, consistency, and currency) and methods for evaluating and enhancing data quality throughout the life of interdependent information systems [1], [2]—dimensions applicable to all aspects of reconciliation in multi-pipeline energy environments. The elastic infrastructure that supports modern release pipelines is driven by research into cloud computing, which was codified in a widely referenced definition which contained the five essential characteristics, the three service models and the four deployment models of cloud computing.

Energy Sector Cybersecurity Research records a growing threat surface in the energy sector, with a focus on SCADA and pipeline telemetry communications, remote terminal units, and industrial control systems, and technical and procedural mitigations relevant for release-time security review [5], [7], [16]. National-level guidance also provides a practical taxonomy of identify, protect, detect, respond, and recover activities in critical-infrastructure cybersecurity risk-management [18] and third-party and vendor risk-scoring studies focus on the dependency and supply-chain aspects of enterprise releases [10].

Governance theory treats information and information technology as artifacts in need of structured decision rights and accountability mechanisms that are separate from those of tangible assets [23], and organizational-culture studies identify generative, bureaucratic, and pathological patterns of how incidents, near-misses, and release failures are reported and addressed [24]. Empirical studies on Methodology (tertiary systematic reviews) also emphasize the need to base governance frameworks on 'cross-study' evidence, rather than on single case reports [11], [25].

These elements—release planning, continuous delivery, data quality, cloud infrastructure, cyber security, governance

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

theory, and organisational culture—are combined in a single, evidence-based assurance model specifically designed for interconnected energy platforms: ERAF.

III. THE ENTERPRISE RELEASE ASSURANCE FRAMEWORK

ERAF organizes release-readiness evaluation into six assurance domains, illustrated in Fig. 1, each of which produces objective evidence that feeds into a composite readiness score.

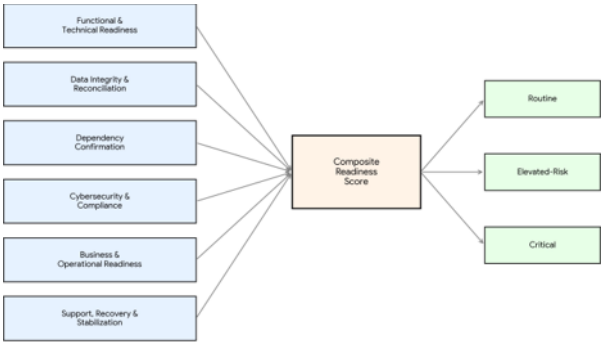

Fig. 1. Six assurance domains feeding a composite release readiness score and tier classification.

Fig. 1. Six assurance domains feeding a composite release readiness score and tier classification.

A. Functional and Technical Readiness

This domain ensures that code changes, configuration changes, and infrastructure changes meet the necessary unit, integration, regression, and performance tests in keeping with continuous-delivery quality-gates documented in previous architecture and practice studies [20], [21]. Subsequent risk scoring is anchored on automated test-pipeline coverage and defect-density metrics recorded at this stage.

B. Data Integrity and Reconciliation

With energy platforms relying on interconnected data pipelines from well and production telemetry systems through to asset, trading, and scheduling operations systems, this domain extends the fundamental data-quality dimensions of accuracy, completeness, consistency and timeliness to ensure that a release does not create reconciliation breaks between upstream and downstream data stores [1], [2]. Evidence is in the form of results from the reconciliation and schema compatibility checks.

C. Dependency Confirmation

With a major release that involves several layers across applications, cloud, database, identity, and API, each of which is managed by an individual team, service, or vendor, the domain formally validates that each team, service, or vendor is compatible – an observation confirmed by the research, as unmanaged cross-team dependency is a top reason for release delay and failure [8], [13], [14].

D. Cybersecurity and Compliance

Documented security review, vulnerability-scan results, and compliance sign-off that meet critical-infrastructure cybersecurity guidance and SCADA/pipeline-control-specific threat-mitigation practices must be obtained for this domain [5], [7], [16], [18]. Third-party and vendor components are also evaluated by employing non-intrusive risk-scoring techniques appropriate to dependency ecosystems that are outside of direct organizational control [10].

E. Business and Operational Readiness

This domain is related to the validation of functional acceptance criteria, communication plans and assessments of impact on field operations and customers, which is an aspect of governance theory's structured decision rights over information assets before deployment [23].

F. Support, Recovery, and Stabilization

The last domain examines if production-support ownership, monitoring thresholds and rollback conditions have

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

been established and practised, and is based on research in the field of organisational culture which has identified that a culture which is generative, as opposed to bureaucratic or pathological, with high information flow and shared responsibility for failure, is more supportive of effective incident recovery [24].

TABLE I SIX ASSURANCE DOMAINS AND THEIR EVIDENTIARY BASIS

Domain	Representative Evidence Artifact	Key Literature
Functional & Technical Readiness	Automated test/regression results; defect density	[9], [20], [21]
Data Integrity & Reconciliation	Reconciliation-run logs; schema compatibility checks	[1], [2]
Dependency Confirmation	Cross-team/vendor sign-off records	[8], [13], [14]
Cybersecurity & Compliance	Vulnerability scans; compliance attestations	[5], [7], [10], [16], [18]
Business & Operational Readiness	Business acceptance sign-off; communication plan	[23]
Support, Recovery & Stabilization	Monitoring thresholds; rollback rehearsal record	[24]

security and compliance are higher for releases that impact pipeline-facing or production data systems [5], [16], [18].

The weighted domain scores are combined into a single composite readiness score, which is then used to classify a release into one of three tiers based on business impact, operational dependency, number of impacted systems, data sensitivity, and the complexity of the rollback, in accordance with previous recommendations that release-planning models should integrate formal scoring with contextual judgment, rather than formal or contextual judgment alone [3], [19], [22].

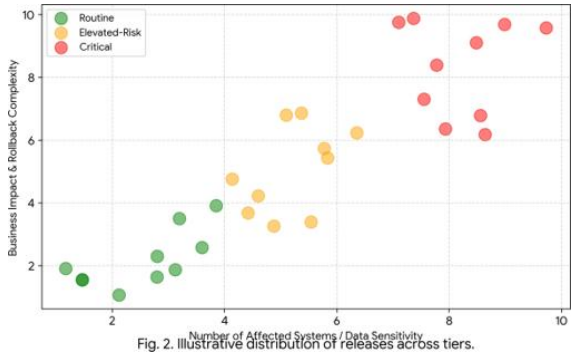

Fig. 2. Illustrative distribution of releases across tiers.

Fig. 2. Illustrative distribution of releases across routine, elevated-risk, and critical tiers.

As shown in Fig. 2, routine releases tend to be focused in the lower left corner, with lower levels of interdependency and complexity in rollback; critical releases tend to be focused in the upper right corner, with higher levels of interdependency and rollback complexity. A sample composite scoring rubric, which operationalizes this classification, is provided in Table II.

TABLE II Illustrative Composite Readiness Scoring Rubric

Domain	Weight (%)	Routine (≥)	Elevated	Critical (<)
Functional & Tech.	20	90	75–89	75
Data Integrity	15	95	85–94	85

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Dependency Conf.	20	90	70–89	70
Cyber & Compliance	25	95	80–94	80
Business & Ops.	10	90	75–89	75
Support & Stab.	10	90	75–89	75

IV. COMPOSITE READINESS SCORING AND RISK

Classification

Each of the six domains in ERAF receives a normalized sub-score, which is illustratively assigned a weight based on the domain's reported impact on release outcomes published in the literature. The weight for functional and functional dependency as well as confirmation of dependency are relatively high because of the relationship with release failures in industrial studies [8], [13], [14], whereas the weights for cyber

The Release Evidence Package

To guarantee that composite scores are based on factual evidence, not on self-reports, ERAF outlines a consistent Release Evidence Package that is to be included with all releases that go beyond the routine tier. The package contains 11 elements as summarized in Fig. 3 and Table III: release scope, affected systems, dependency confirmation, testing results, data-validation records, security approval, cutover plan, business validation, monitoring thresholds, support ownership, and rollback conditions.

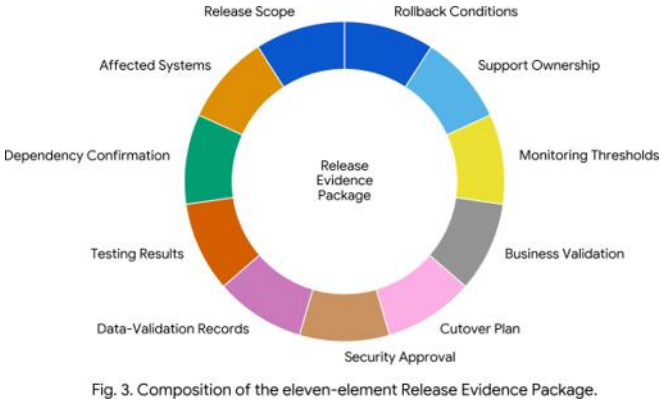

Fig. 3. Composition of the eleven-element Release Evidence Package.

Fig. 3. Composition of the eleven-element Release Evidence Package.

The structured, traceable release artifacts, as well as ex-plicit rollback conditions and monitoring thresholds, are very similar to automated release-note generation studies, which have found that structured and traceable release artifacts can be assembled from existing development-lifecycle records, instead of being manually written, and to continuous-delivery studies, which have named inadequate rollback and monitoring preparation as recurring causes of release failure. Filling in the package also facilitates tertiary review processes as suggested by methodological guidelines for governance evidence aggregation across releases for subsequent empirical analysis [11], [25].

Table Iii Release Evidence Package Elements

Element	Purpose	Related Domain
Release Scope	Defines boundaries of the change set	Functional & Technical

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Affected Systems	Enumerates all downstream/upstream systems touched	Dependency Confirmation
Dependency Confirmation	Records sign-off from dependent teams/vendors	Dependency Confirmation
Testing Results	Documents test coverage and outcomes	Functional & Technical
Data-Validation Records	Confirms reconciliation and schema integrity	Data Integrity
Security Approval	Confirms vulnerability scan and compliance sign-off	Cybersecurity & Compliance
Cutover Plan	Details deployment sequencing and timing	Functional & Technical
Business Validation	Confirms stakeholder acceptance	Business & Operational
Monitoring Thresholds	Defines post-release alerting criteria	Support & Stabilization
Support Ownership	Assigns accountable on-call personnel	Support & Stabilization
Rollback Conditions	Specifies triggers and steps for reversal	Support & Stabilization

V. LEADING RISK INDICATORS

Given that composite readiness scores are by definition backward looking in that they will reflect evidence gathered up until the point at which they are scored, ERAF adds seven leading risk indicators that will help to bring to light any emerging risk before release: unresolved dependency age, late scope changes, failed integration tests, defect reopening, approval delays, incomplete rollback preparation, and insufficient production support. Each of these indicators is defined in Table IV and a typical indicator profile for routine and critical releases is compared in Fig. 4.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The critical releases have very high values on all seven indicators compared to the routine releases, as seen in Fig. 4. These indicators are based directly on documented predictors of release difficulty, such as unmanaged dependency [8], [14], and patterns of defects and rework caused by insufficiently automated pipelines [9], [20] and inadequate production-support staffing associated with prolonged post-release stabilization [21], [24].

VI. EVALUATION METRICS AND EMPIRICAL DISCUSSION

ERAF is evaluated using seven outcome metrics: deployment frequency, change-failure rate, escaped defects, emergency-release frequency, rollback rate, stabilization du-ration, and release predictability. These metrics align closely with continuous-delivery evaluation criteria established in prior systematic reviews of CI/CD adoption [20], [21] and with empirical comparisons of release-engineering maturity across organizations of different scale [13].

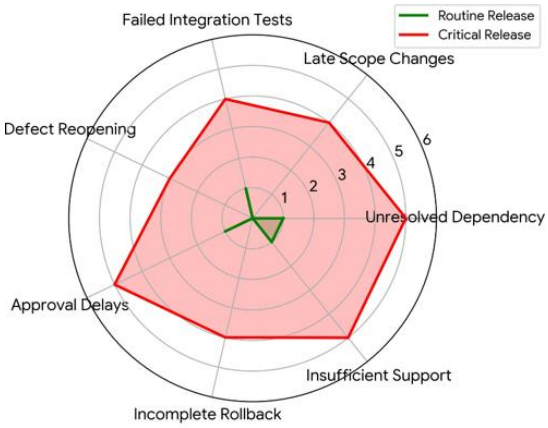

Fig. 4. Illustrative leading risk indicator profiles.

Fig. 4. Illustrative leading risk indicator profiles for routine versus critical releases.

TABLE IV Leading Risk Indicators and Illustrative Escalation Thresholds

Indicator	**Definition**	**Illustrative Threshold**
Unresolved Dependency Age	Days a cross-team dependency remains unconfirmed	> 5 business days
Late Scope Changes	Scope changes introduced after code freeze	> 2 changes
Failed Integration Tests	Share of integration test suite failing on first run	> 10%
Defect Reopening	Defects reopened after prior closure	> 3 defects
Approval Delays	Days beyond target for required sign-off	> 3 business days

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Incomplete Rollback Prep.	Rollback steps untested prior to release	Any untested step
Insufficient Prod. Support	Support staffing below planned on-call level	< 80% of planned staffing

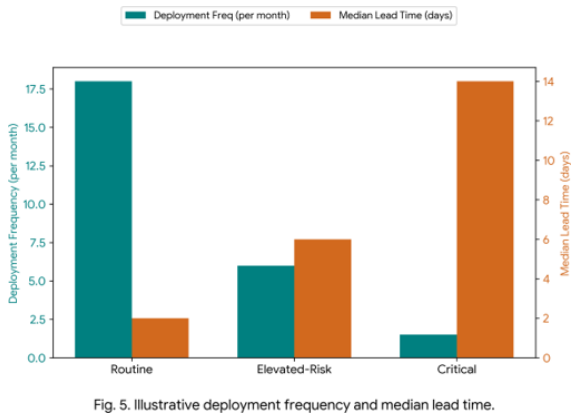

Fig. 5. Illustrative deployment frequency and median lead time.

Fig. 5. Illustrative deployment frequency and median lead time by release tier.

Fig. 5 presents illustrative deployment frequency and median lead time by release tier, showing that routine releases can be delivered substantially more frequently and with shorter lead time than critical releases, reflecting the additional evidentiary and review burden the latter incur under ERAF.

For illustrative purposes, Fig. 6 shows failure and rollback rates for each tier; there is a higher failure rate and a higher rollback rate for critical releases, reflecting the fact that they are more extensive and interdependent, the basis for the more extensive Release Evidence Package and leading indicator monitoring applied to this tier. Table V shows the tiers compared for all seven evaluation metrics.

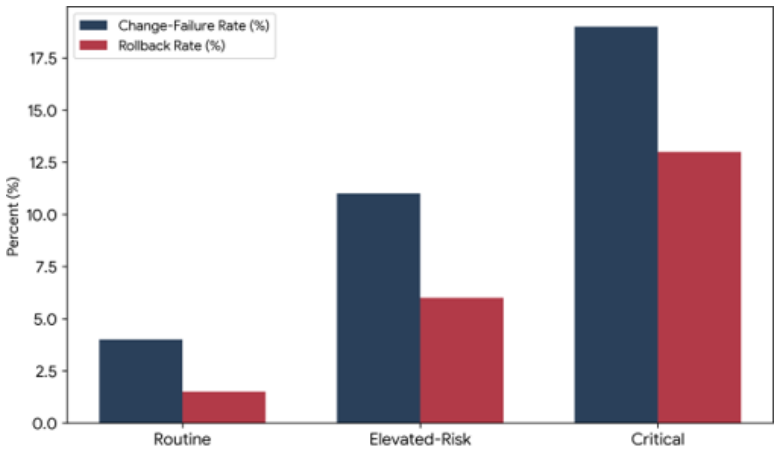

Fig. 6. Illustrative change-failure rate and rollback rate.

Fig. 6. Illustrative change-failure rate and rollback rate by release tier.

Differentiated assurance intensity (lighter for routine releases, progressively heavier for releases with elevated risk and critical releases) provides a way to progressively raise the speed of delivery while not easing up on the governance uniformly, a dynamic that has been repeatedly observed in studies about adoption of continuous delivery [4], [12] and has been dubbed as the technical-social tension between speed and control.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

TABLE V **Illustrative Evaluation Metrics by Release Tier**

Metric	Routine	Elevated-Risk	Critical
Deployment Freq. (per month)	18	6	1.5
Change-Failure Rate (%)	4	11	19
Escaped Defects (per release)	0.8	2.1	4.3
Emergency Releases (%)	1	4	9
Rollback Rate (%)	1.5	6	13
Stabilization Duration (hours)	4	18	48
Release Predictability (%)	96	84	71

VII. COMPARATIVE ANALYSIS ACROSS RELEASE TIERS

The table below also shows, on four qualitative-quantitative dimensions, the typical dependency count, security-review depth, business-validation scope, and stabilization staffing for the three release tiers.

The comparison shows that there is a need for more dependency confirmation and more security review depth in elevated-risk and critical releases, which aligns with the findings of cross-team/cross-vendor dependency as the primary factor that affects release risk in complex socio-technical systems [8], [10], [13], [14].

The comparison also shows that the number of stabilization staffing (production support staff during the post-release window) is scaled with tier, which is in line with organizational-culture research linking sufficient support staffing and information flow with promptness of incident detection and recovery [24].

The collective results indicate that a tiered assurance model is more representative of the actual level of risk, and thus more appropriate than a single release process, which is consistent with decades of release-planning research that warns against"one size fits all" release processes [6], [19], [22].

TABLE VI COMPARATIVE QUALITATIVE-QUANTITATIVE PROFILE BY RELEASE TIER

Dimension	Routine	Elevated-Risk	Critical
Typical Dependency Count	1–2	3–6	7+
Security-Review Depth	Automated scan only	Manual + automated review	Full review + third-party risk scoring
Business-Validation Scope	Product-owner sign-off	Sign-off + user acceptance testing	Sign-off + UAT + executive briefing

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Stabilization Staffing	On-call engineer	Dedicated support pair	Cross-functional stabilization team

VIII. CONCLUSION AND FUTURE DIRECTIONS

This paper has presented a new governance framework for releases from interconnected energy data, cloud, and application platforms, called the Enterprise Release Assurance Framework, that combines research on release planning, continuous delivery, data quality, cybersecurity, governance theory, and organisational culture to provide a coordinated approach to releases. The framework establishes readiness evaluations across six assurance domains, combines evidence across the domains into a composite, tiered readiness score, creates a standard Release Evidence Package, and tracks leading risk indicators, as well as outcome measures, during the process, providing energy enterprises with a way to accelerate delivery while delivering a proportionate level of operational, security, and data integrity risk.

The synthesis here is conceptual, and the example scoring rubrics, thresholds, and metric values in Tables II-VI are only illustrative of the structure of the framework and do not represent industry-validated metrics or scores.

Based on the literature reviewed in this paper, future studies should seek to validate ERAF in operating energy enterprises by tracking the seven evaluation metrics over the course of time for each release of the framework; investigate the domain weights through a statistical analysis of historical results of releases; and expand the domain of data-integrity into real-time and streaming data-reconciliation domains to meet evolving requirements of real-time and streaming energy enterprise data sources.

REFERENCES

[1] C. Batini and M. Scannapieco, Data Quality: Concepts, Methodologies and Techniques. Berlin, Germany: Springer, 2006.

[2] C. Batini and M. Scannapieco, Data and Information Quality: Dimensions, Principles and Techniques. Cham, Switzerland: Springer, 2016.

[3] H. C. Benestad and J. E. Hannay, “A comparison of model-based and judgment-based release planning in incremental software projects,” in Proc. 33rd Int. Conf. Software Engineering, 2011, pp. 766–775.

[4] G. G. Claps, R. Berntsson Svensson, and A. Aurum, “On the journey to continuous deployment: Technical and social challenges along the way,” Inf. Softw. Technol., vol. 57, pp. 21–31, 2015.

[5] D. Faquir, N. Chouliaras, V. Sofia, K. Olga, and L. Maglaras, “Cybersecurity in smart grids, challenges and solutions,” AIMS Electron. Electr. Eng., vol. 5, no. 1, pp. 24–37, 2021.

[6] D. Greer and G. Ruhe, “Software release planning: An evolutionary and iterative approach,” Inf. Softw. Technol., vol. 46, no. 4, pp. 243–253, 2004.

[7] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” Comput. Netw., vol. 169, art. 107094, 2020.

[8] S. Jantunen, L. Lehtola, D. C. Gause, U. R. Dumdum, and R. J. Barnes, “The challenge of release planning,” in Proc. 5th Int. Workshop Software Product Management, 2011, pp. 36–45.

[9] T. Karvonen, W. Behutiye, M. Oivo, and P. Kuvaja, “Systematic literature review on the impacts of agile release engineering practices,” Inf. Softw. Technol., vol. 86, pp. 87–100, 2017.

[10] O. F. Keskin, K. M. Caramancion, I. Tatar, O. Raza, and U. Tatar, “Cyber third-party risk management: A comparison of non-intrusive risk scoring reports,” Electronics, vol. 10, no. 10, art. 1168, 2021.

[11] B. Kitchenham et al., “Systematic literature reviews in software engineering—A tertiary study,” Inf. Softw.

Technol., vol. 52, no. 8, pp. 792–805, 2010.

[12] E. Laukkanen, J. Itkonen, and C. Lassenius, "Problems, causes and solutions when adopting continuous delivery—A systematic literature review," Inf. Softw. Technol., vol. 82, pp. 55–79, 2017.

[13] E. Laukkanen, M. Paasivaara, J. Itkonen, and C. Lassenius, "Comparison of release engineering practices in a large mature company and a startup," Empir. Softw. Eng., vol. 23, no. 6, pp. 3535–3577, 2018.

[14] M. Lindgren, R. Land, C. Norstro¨m, and A. Wall, "Key aspects of software release planning in industry," in Proc. 19th Australian Conf. Software Engineering, 2008, pp. 320–329.

[15] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2011.

[16] F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," Energies, vol. 14, no. 5, art. 1380, 2021.

[17] L. Moreno et al., "ARENA: An approach for the automated generation of release notes," IEEE Trans. Softw. Eng., vol. 43, no. 2, pp. 106–127, 2017.

[18] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity," Version 1.1, Gaithersburg, MD, USA, 2018.

[19] G. Ruhe and A. Ngo-The, "Hybrid intelligence in software release planning," Int. J. Hybrid Intell. Syst., vol. 1, no. 2, pp. 99–110, 2004.

[20] M. Shahin, M. A. Babar, and L. Zhu, "Continuous integration, delivery and deployment: A systematic review on approaches, tools, challenges and practices," IEEE Access, vol. 5, pp. 3909–3943, 2017.

[21] M. Shahin, M. Zahedi, M. A. Babar, and L. Zhu, "An empirical study of architecting for continuous delivery and deployment," Empir. Softw. Eng., vol. 24, no. 3, pp. 1061–1108, 2019.

[22] M. Svahnberg et al., "A systematic review on strategic release planning models," Inf. Softw. Technol., vol. 52, no. 3, pp. 237–248, 2010.

[23] P. P. Tallon, R. V. Ramirez, and J. E. Short, "The information artifact in IT governance: Toward a theory of information governance," J. Manage. Inf. Syst., vol. 30, no. 3, pp. 141–178, 2013.

[24] R. Westrum, "A typology of organisational cultures," Qual. Saf. Health Care, vol. 13, suppl. 2, pp. ii22–ii27, 2004.

[25] L. Zhang, J.-H. Tian, J. Jiang, Y.-J. Liu, M.-Y. Pu, and T. Yue, "Empirical research in software engineering—A literature survey," J. Comput. Sci. Technol., vol. 33, no. 5, pp. 876–899, 2018.