Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(12), 9-27
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Convergence of Cybersecurity Governance, Risk Management and Compliance (GRC) for IT and OT Environments - Context of KSA

Muhammad Shoaib, Abdulaziz Alharbi

Department of Information Technology, Preston University, Islamabad, Pakistan
Email: Shoaib.sheikh1@gmail.com, abdulaziz2alharbi@gmail.com

How to cite this paper: Shoaib, M. and Alharbi, A. (2025) Convergence of Cybersecurity Governance, Risk Management and Compliance (GRC) for IT and OT Environments - Context of KSA. *Journal of Computer and Communications*, **13**, 9-27.
https://doi.org/10.4236/jcc.2025.1312002

Received: November 7, 2025
Accepted: December 14, 2025
Published: December17, 2025

Abstract

The growing convergence of Information Technology (IT) and Operational Technology (OT) has introduced complex cybersecurity, governance, and compliance challenges for organizations, particularly within the Kingdom of Saudi Arabia (KSA). This study addresses these challenges by proposing an Integrated IT-OT Governance, Risk, and Compliance (I-GRC) Framework that unifies cybersecurity management across both domains. Using a descriptive analytical approach, this research reviewed scholarly literature published between 2020 and 2025 from leading databases, including JSTOR, Taylor & Francis Online, Emerald Insight, ScienceDirect, IEEE Xplore, and SpringerLink. It also examined key international standards—ISO/IEC 27001, ISA/IEC 62443, and NIST SP 800-82—to identify common control objectives, risk models, and compliance practices relevant to IT-OT integration. The findings and synthesis of twelve recent peer-reviewed studies led to the development of the I-GRC Framework, built around four core determinants: Governance Integration, Risk Management Alignment, Compliance Harmonization, and Performance Measurement. These determinants collectively ensure consistent leadership, unified risk assessment, streamlined compliance across IT and OT domains, and continuous evaluation through measurable cybersecurity indicators. Aligned with the National Cybersecurity Authority (NCA) guidelines and Vision 2030 objectives, the proposed I-GRC Framework enhances Saudi Arabia's national cybersecurity posture by promoting regulatory readiness, operational resilience, and data-driven governance. The study contributes a practical and measurable model for organizations seeking to bridge IT and OT systems, improve compliance maturity, and achieve sustainable cybersecurity integration within critical infrastructure sectors.

Keywords

IT-OT Convergence, I-GRC Framework, Cybersecurity Governance, ISO/IEC 27001, ISA/IEC 62443, NIST SP 800-82, Saudi Arabia, Vision 2030

1. Introduction

In today's hyperconnected industrial landscape, the convergence of Information Technology (IT) and Operational Technology (OT) has become a strategic necessity for organizations aiming to achieve comprehensive cybersecurity resilience. The growing number of IT systems, which process data and business processes, interconnecting with the OT environments, which control industrial control systems (ICS), has increased the cybersecurity threat area significantly. The report by IBM on the Cost of a Data Breach 2024 reported that the average cost of a data breach was USD 4.88 million in 2024, an increment of 10 per cent over 2023 [1]. Effects of cyberattacks in critical sectors like energy and manufacturing are even more far-reaching since they do not only pose a threat to financial stability but also operational sustainability and the safety of people. Therefore, it is necessary to create a consistent Governance, Risk and Compliance (GRC) framework which will incorporate both IT and OT cybersecurity needs, especially in the jurisdictions where rapid digital and industrial transformation is occurring, such as the Kingdom of Saudi Arabia (KSA).

1.1. Background

The Kingdom of Saudi Arabia has been at the forefront of digital transformation through its Vision 2030 initiative, which emphasizes industrial automation, smart manufacturing, and critical infrastructure modernization. This increased digitization has, however, increased the threat of cyber-attacks not only on IT but also on OT systems. The National Cybersecurity Authority (NCA) said that cyber-attacks on vital sectors increased by 56 percent from 2022 to 2024 [2]. Besides, as per Kaspersky (2024), Saudi Arabia has 7.8% of all industrial control systems (ICS) cyber incidents that are reported in the Middle East, which is highly vulnerable in the field of transformation into Industry 4.0 [3].

The integration of IT and OT space requires a common approach to governance and compliance in the field of cybersecurity. Conventional IT models, including the ISO/IEC 27001, tend to be a solid ground in dealing with security risks, yet they frequently lack the details regarding industrial systems of automation. On the other hand, other OT frameworks like the ISA/IEC 62443 are typically focused on operational safety, asset integrity, and control network segmentation but have few opportunities to cover enterprise-wide risk governance. A combination of IT and OT GRC helps organizations to streamline the technical controls, promote regulatory compliance, and streamline their incident response strategies.

The regulatory alignment in KSA is initiated by different international and na-

tional standards, such as ISO/IEC 27001, ISA/IEC 62443, and NIST SP 800-82, which collectively cover the entire scope of IT governance as well as the operational security of OTs. The NIS2 Directive of the European Union, as well as the NERC CIP standards of North America, can also be seen as an example of the international movement towards the more harmonized regulatory framework, which requires organizations to implement integrated Compliance Frameworks. Sector-specific controls based on these international standards have been proposed by the Saudi NCA and facilitating interoperability and resilience in the national critical infrastructure systems [4].

Despite these advancements, many organizations still face challenges in mapping overlapping controls, ensuring cross-domain visibility, and aligning cybersecurity metrics between IT and OT ecosystems. This research therefore proposes a single, implementable IT-OT-GRC framework, tailored to the Saudi context, to harmonize governance structures, standardize risk assessment methodologies, and enable a coherent approach to cybersecurity management across industrial and enterprise domains. Through detailed mapping of standards, gap analysis, and real-world sectoral case studies, this paper aims to provide both strategic and operational insights for practitioners and policymakers seeking to strengthen cybersecurity convergence in the Kingdom's evolving digital economy.

1.2. Problem Statement

Organizations in critical sectors such as energy, manufacturing, and utilities increasingly operate converged IT and OT systems, yet their Governance, Risk, and Compliance (GRC) functions remain largely siloed. This lack of unified GRC oversight creates a core practical problem: disjointed governance structures, inconsistent risk assessment methods, and fragmented compliance processes, which lead to duplicated controls, unclear accountability, and delayed or ineffective incident response across IT-OT environments. These issues ultimately heighten the likelihood and impact of cyber incidents on safety-critical industrial processes [5].

Despite the literature records of technical and organizational motivations behind IT/OT integration, an ongoing void of implemented, evidence-based frameworks, which 1) aligns control goals between ISO/IEC 27001 and ISA/IEC 62443, 2) translates OT oriented metrics of safety to enterprise GRC dashboards, and 3) offers validated and implementable mapping templates and methods to measurement, exists [6]; mapping studies on IEC 62443. Some prevailing reviews and guidelines on standards describe how to align and not go beyond that, without providing reproducible, sector-specific GRC artefacts and validated processes of gap analysis that can be used by practitioners within national regulatory frameworks like the Kingdom of Saudi Arabia.

This paper thus seeks to fulfill the practical value of a unified application executable IT-OT-GRC framework such as 1) integrating standards and scholarly data into harmonized control goals, 2) generating mapping templates and metrics, and 3) testing them on sectoral case studies - bridging the gap between the high-

level standards and the application.

1.3. Research Objectives

To develop a unified IT-OT Governance, Risk, and Compliance (GRC) framework that harmonizes international standards such as ISO/IEC 27001, ISA/IEC 62443, and NIST SP 800-82, addressing both enterprise-level and industrial cybersecurity requirements in the context of Saudi Arabia's critical infrastructure sectors.

1.4. Significance of Research

The research is important as it will fill a serious gap between enterprise IT governance and industrial OT cybersecurity in the rapidly developing digital landscape of Saudi Arabia. With the implementation of Industry 4.0 in organizations, the risk of cross-domain cyber-attacks increases, and this is why a single Governance, Risk and Compliance (GRC) framework is necessary. The paper is both academically and practically pertinent since it incorporates internationally agreed standards, such as ISO/IEC 27001, ISA/IEC 62443 and NIST SP 800-82, in a scalable and context-specific model applicable to the Saudi Arabian critical infrastructure industries.

Academically, this study contributes to the research on IT-OT convergence through hypotheses of measurable indicators to evaluate IT cybersecurity maturity and risk alignment and harmonization of control. In practice, it provides policymakers, regulators, and cybersecurity leaders with a systematic approach of assessment and reinforcement of compliance and resilience in national infrastructure. Using descriptive data analysis, the study also offers empirical support of effectiveness of the framework, facilitates the use of data in decision-making and benchmarking of organizations. Finally, the study is in line with the objectives of the Saudi Arabia Vision 2030 concerning the development of cybersecurity capabilities at the national level, the continuity of operations, and the development of technology, hence, supporting the national security and sustainable growth of the economy.

2. Literature Review

This chapter provides a comprehensive review of existing academic and professional literature related to the convergence of Information Technology (IT) and Operational Technology (OT) within Governance, Risk, and Compliance (GRC) frameworks, with a specific focus on cybersecurity integration in critical infrastructure sectors. This review aims to investigate the theoretical backgrounds, practice, and empirical evidence that can be used to develop a standardized approach to IT-OT-GRC that can be effective in the Kingdom of Saudi Arabia (KSA). Literature review will be based on peer-reviewed scholarly databases like JSTOR, Taylor and Francis online, Emerald Insight, ScienceDirect, IEEE Xplore and SpringerLink in order to achieve academic rigor and relevance. Conceptual

and empirical literature is reviewed to learn about the development of standards like ISO/IEC 27001, ISA/IEC 62443 and NIST SP 800-82, and their overlaps as a part of integrated governance models. The following sections will synthesize the literature thematically, highlighting the current state of IT-OT convergence, identifying challenges in harmonizing cybersecurity controls, and outlining the research gaps that justify the need for this study's proposed framework.

2.1. Cybersecurity Governance

Cybersecurity governance has developed into a specific area of convergence between corporate governance and risk management and technical cyber defense. The initial governance practices focused on board accountability and technical risk translation into strategic decision-making [7]. The convergence between the IT and OT domain has seen the governance field grow to consider organizational structures, metrics and learning mechanism that moulds cyber resilience across the socio-technical systems.

Recent empirical research is concerned with the impact of governance structure, board participation, and accountability design on an organization to deal with cyber risk. Research by Gale *et al.* (2022) in the framework of corporate boards and senior management applied semi-structured interviews and mixed-method analysis to identify the drivers and barriers to board engagement; the findings show that inadequate cyber literacy, inappropriate measurement of reporting, and unclear accountability hinder effective oversight [8]. In the same vein, Cortez and Dekker (2022) explored the practices of semi-structured interviews with C-suite practitioners in the financial sector to study cybersecurity disclosure practices within the sector, the authors note that agency problems and information asymmetries are the main obstacles to transparent governance and meaningful disclosure [7].

Field research focuses on various governance levers. Slapničar *et al.* (2023) conducted a detailed field research on accountability configurations, i.e. operationalizing Five Lines of Accountability; they used qualitative case analysis to demonstrate that separate role separation (with an involved board) is associated with a more consistent cyber processes, but they also discovered that organizations tend to blur lines in order to be more efficient at the cost of clarity of oversight [9]. Conversely, Patterson *et al.* (2024) applied qualitative interviews (n = 34 individuals working in the field of security) to study organizational learning following cyber incidents; the authors conducted the study based on the idea that, despite the presence of governance structures, organizational learning and resiliency are restricted by cultural barriers and superficial post-incident reviews [10].

Sector- and domain-focused surveys add further nuance. In a survey of the energy/ICS domain, Boeding *et al.* (2022) synthesized standards and countermeasures and revealed that OT, in line with IT-centric confidentiality-based models, makes trade-offs in governance, as described by its priorities (availability and safety). Their analysis and synthesis (on the basis of literature and standards map-

ping) are that governance models need to be tailored to operational limits related to the domain and that generalized governance results in inappropriate controls [11].

These studies all lead to converging around three themes: 1) There must be board and executive engagement, which is typically hindered by insufficient metrics and cyber literacy [7] [8]; 2) explicit accountability frameworks (e.g., Five Lines) are the way to enhance governance clarity, but the problem is that such models are not generally or neatly adopted [9]; and 3) domain-specific tensions (IT vs O Empirically, it still requires quantifiable, implementable artefacts of governance the standardized metrics, cross-domain mappings, and tested and post-incident learning processes that can be operationalized and evaluated across sectors. This gap is the reason why the current study is specifically interested in an operation IT-OT-GRC framework that is not only measurable by descriptive analysis but is also responsive to the specifics of the domain.

2.2. Governance, Risk Management and Compliance

Governance, Risk Management and Compliance (GRC) has evolved from an independent corporate initiative to a combined discipline to help synchronize the strategy, controls and regulatory demands of organizations. Initial conceptual literature conceptualized GRC as an organization-wide competency that aligns goals and risk tolerance and risk management requirements by claiming that the siloed methods create inefficiency and blind spots [12]. In the past ten years, the focus of research has moved towards relevant models, maturity measurement, and empirical validation of combination GRC models, particularly in situations where risk is increased by digitalization and regulatory complexity.

One of the earliest studies by Racz *et al.* (2010) created a frame of reference of integrated GRC through a synthesis of literature and a survey of practitioners; their article suggested conceptual building blocks (governance, risk processes, compliance mapping, and supporting information architecture) and the importance of data-based reference models in operationalizing GRC at the business and IT levels [12]. On top of that background, empirical studies have delved into the issue of using maturity models and standards-based controls to aid in measurement and alignment. As an example, Schmitz *et al.* (2021) examined the practitioners maturity-level capacity to assess information-security controls: on the basis of the empirical case assessments with security experts, they revealed that although maturity models are common, the quality of the estimates made by practitioners significantly varies, and the quality of the assessment depends on the clear operational criteria and expertise of assessors [13].

Recent studies on the comparative framework provide complementary studies. Comparing the most popular cybersecurity/GRC frameworks (e.g., COBIT, ISO/IEC 27001, NIST variants, and more recent standards) through content-analytic and expert-validated methods, McIntosh *et al.* (2024) show that each framework focuses on different areas, and the integration of multiple frameworks would help

organizations to cover the areas of governance, risk, and compliance in an inclusive manner. Their qualitative study suggested the practical mapping layers and expert in the loop validation on the framework adaptation to the new technologies [14]. Conversely, the enterprise-governance effort by De Haes and Van Grembergen (2015) focuses more on the mechanisms of institutional design and alignment (board roles, IT decision rights, performance metrics) and holds that the effectiveness of the GRC integration also relies not on technical control mappings alone, but equally on governance arrangements and accountability lines [15].

All these studies come together on three factual points: 1) conceptual models of integrated GRC are developed and useful in organizing research and practice [12]; 2) maturity models and control assessments are useful but generate inconsistent results unless the operational definitions and assessment training is standardized [13]; and 3) comparative framework studies and governance scholarship show that in order to succeed in making integrated GRC work, the alignment of governance structures, methodological approaches of control, and mapping of frameworks has to Nevertheless, there is still a perceived practical gap: little of the literature generates validated, sector-specific, implementable mapping artefacts (control-overlap ratios, standardized maturity questionnaires, or descriptive baselines) that can be used and measured by practitioners through descriptive analysis of data. The paper fulfills that void by suggesting a working IT-OT-GRC framework with indicators that can be measured and testing its implementation and success in critical sectors of KSA.

2.3. IT-OT Environment

IT-OT environment defines the interface between enterprise Information Technology (IT) which is about data, applications and business processes and Operational Technology (OT) which is about control systems, field devices and real time industrial processes. With the spreading use of Industry 4.0 and IIoT (Industrial Internet of Things) platforms, formerly air-gapped OT systems are becoming networked with IT and result in new efficiencies, y*et al*so cyber-physical vulnerabilities [16]. The IT-OT interactions area of research has been researched on architecture, interoperability, risk, and organizational change, with scholars pointing out that technical integration is to be accompanied by governance and process adjustment.

An IIoT analysis framework study by Boyes *et al*. (2018) is designed to describe devices, layers, and threats in the industrial architectures. To map components of IIoT and uncover security and interoperability vulnerabilities, authors performed a comprehensive literature review and architectural analysis and found that IIoT raises the attack surface especially at protocol and gateway layers and that the taxonomy-based analysis can help to select a targeted control [17]. Humayed *et al*. (2017) conducted a survey of the state of cyber-physical systems (CPS) security in representative fields (smart grid, medical CPS, smart vehicles) to systematize

threats, vulnerabilities, attacks and defenses; their synthesis emphasizes that the heterogeneity and real-time safety demands of OT make the application of IT security practices more difficult [16].

Empirical research of IT-OT convergence provides organizational and adoption in perspectives. Ehie and Chilton (2020) performed an empirical study of manufacturing organizations by conducting a survey and regression analysis to test a two-stage model of the relationship between IT-OT convergence to the adoption of IoT. According to their survey, the alignment between IT and OT (similar goals, governance) in an organization is a significant predictor of successful IoT adoption, although technological legacy and skills gap moderate this association [18]. Conversely, Yaacoub *et al.* (2020) offer a wide overview of CPS security restrictions and future developments, conducting a systematic literature review study, and point out that a significant part of mitigation strategies are still at the stage of proof-of-concept and have not been proven in actual OT environments; they state that real, domain-sensitive defenses and testbeds are still required to close the research-to-practice gap [19].

3. Materials and Methods

The research design is descriptive in the study in order to establish a single Governance, Risk, and Compliance (GRC) framework of IT-OT convergence in the context of the Kingdom of Saudi Arabia (KSA). The study solely uses secondary data sources, including mostly peer-reviewed academic reports and official reports, and international standards on cybersecurity. The reason why the descriptive approach is selected is that it is possible to conduct systematic observation, classification, and synthesis of available empirical data to discover patterns, gaps, and best practices applicable to IT-OT governance integration.

The source material to use in this research was gathered in this study through reputable academic databases namely, JSTOR, Taylor and Francis Online, Emerald Insight, ScienceDirect, IEEE Xplore and springer link. These databases were chosen because they have a wide range of peer review journals and conference papers in areas of information security, industrial automation and governance research. To guarantee the currency and relevance of the findings, literature search was limited to the studies published after 2020 and till 2025. The keywords included IT-OT convergence, cybersecurity governance, GRC frameworks, risk management, and industrial control systems security in different combinations to get the relevant studies.

The pre-screening on titles and abstracts was conducted on about 30 peer-reviewed studies. The inclusion criteria stipulated that any study 1) was dealing with at least one of the dimensions of governance, risk, or compliance in IT-OT environments, 2) provided empirical figures or theoretical perspectives, and 3) provided information that was relevant to any critical infrastructures like energy, manufacturing, or utilities. Using these criteria, 12 studies were chosen to be analyzed in their full text.

A descriptive analytical approach is the most appropriate method for this study because the primary objective is to develop a conceptual and integrative GRC framework for IT-OT convergence, which requires synthesizing diverse theoretical models, international standards, and empirical findings rather than collecting new field data. Existing frameworks such as ISO/IEC 27001, ISA/IEC 62443, and NIST SP 800-82 are already well-established, and understanding how they can be harmonized demands comparative analysis, cross-mapping, and thematic synthesis, rather than survey-based or case-based empirical work. Additionally, because IT-OT convergence in Saudi Arabia is still emerging, organizations often restrict disclosure of operational and security data, making surveys or early case studies less feasible and vulnerable to incomplete or biased responses. A literature-driven descriptive approach, therefore, provides a broader and more reliable evidence base, allowing the study to integrate international best practices, highlight gaps, and develop a theoretically grounded I-GRC framework that can later be empirically validated. This method ensures conceptual rigor and positions the research for future quantitative or case-based testing once the proposed framework is established.

A thematic synthesis method was used in the analysis, in which all the results of each study were grouped as either governance integration, risk management alignment, compliance harmonization, or performance measurement. Summative analysis was subsequently used to generalize recurring concepts, structures, processes and measures. It was found that there are trends in the implementation and harmonization of existing standards, like ISO/IEC 27001, ISA/IEC 62443 and NIST SP 800-82 across IT and OT systems.

Through these insights synthesized, the study came up with the Integrated IT-OT Governance, Risk, and Compliance (I-GRC) Framework, which is specific to the cybersecurity and industrial context of Saudi Arabia. The framework focuses on quantifiable measures like level of compliance maturity, rate of reduction of incidents and ratio of control overlap.

The proposed methodological approach allows guaranteeing that the model suggested is evidence-based, analytically grounded, and contextually oriented towards the objectives of the Vision 2030 of the Saudi Arabian context. It fills the knowledge gap between theoretical concepts and the actual application and offers a solid base to the policymakers and practitioners to enhance IT-OT cybersecurity governance in the critical infrastructure.

4. Results and Discussion

This chapter summarizes and discusses the results of the descriptive analysis of the peer-reviewed articles on IT -OT convergence and Governance, Risk, and Compliance (GRC) integration. The findings present major patterns, frameworks, and best practices that are determined considering the recent literature published in 2020-25. Patterns were observed in the implementation and harmonization of the existing standards like ISO/IEC 27001, ISA/IEC 62443 and NIST SP 800-82

between IT and OT systems. The discussion also relates the findings to the cyber-security and regulatory environment of Saudi Arabia, showing that it has been used to shape and confirm the design of the proposed Integrated IT -OT GRC Framework (I-GRC). Using descriptive analysis and review analysis of standards a framework is suggested.

4.1. Thematic Synthesis

Table 1 below is the meta-analysis:

Table 1. Meta analysis.

#	Title (Author, Year)	Aim of research	Relation with standards	Key themes (Governance Integration; Risk Mgmt Alignment; Compliance Harmonization; Performance Measurement)
1	Cyber-physical systems security: Limitations, issues and future trends [19]	Systematic survey of CPS/IIoT threats, vulnerabilities and defenses.	Compares CPS security practices against standards such as NIST guidance and IEC/ISA 62443.	Governance: calls for cross-domain governance; Risk: heterogeneity complicates risk models; Compliance: gaps between IT standards and OT requirements; Performance: lack of validated OT metrics.
2	Industrial IoT, Cyber Threats, and Standards Landscape [20]	Map IIoT threat landscape and evaluate standards coverage.	Explicit mapping of ISO/IEC 27001, IEC 62443 and others.	Governance: recommends mapping ISMS to OT program; Risk: taxonomy for IIoT risks; Compliance: roadmap to harmonize multiple standards; Performance: proposes measurable roadmaps (patching, inventory rates).
3	IIoT-ARAS: IIoT/ICS automated risk assessment system [21]	Design and evaluation of an automated risk-assessment tool for IIoT/ICS.	Implements OCTAVE Allegro/references ISO/IEC 27030 (draft) for assessment logic.	Governance: supports decision automation and operator dashboards; Risk: automated scoring of IT/OT exposures; Compliance: enables mapping outputs to standards; Performance: predictive risk KPIs and detection metrics.
4	Survey of cybersecurity governance, threats, and countermeasures for the power grid [11]	Review governance and countermeasures for power-grid ICS/OT.	Discusses NERC CIP, IEC 62443, NIST CSF/SP mappings.	Governance: sectoral governance constraints and operator responsibilities; Risk: critical-infrastructure risk prioritization; Compliance: sectoral standard compliance needs; Performance: operational metrics (detection, patching).
5	Governing cybersecurity from the boardroom [8]	Explore board engagement and oversight practices in cybersecurity.	Relates board reporting to ISO/IEC 27001 reporting requirements and CS frameworks.	Governance: highlights weak cyber literacy at board level (need for integrated reporting); Risk: inconsistent reporting metrics hamper integrated risk view; Compliance: disclosure gaps; Performance: argues for board KPIs and dashboards.

Continued

6	Maturity level assessments of information security controls [13]	Empirical analysis of practitioners' ability to assess control maturity.	Uses maturity models commonly linked to ISO/IEC 27001 assessments.	Governance: need for trained assessors and governance of assessment process; Risk: assessor variability undermines risk baselines; Compliance: measurement ambiguity; Performance: validates maturity scoring but warns about inter-rater reliability.
7	A pathway model to five lines of accountability in cybersecurity governance [9]	Field study on accountability configurations (Five Lines model).	Focuses on governance models (fits with audit/assurance frameworks).	Governance: clear role separation improves oversight; Risk: clarified responsibilities lead to better risk ownership; Compliance: streamlined audit trails; Performance: accountability metrics improve remediation speed.
8	Security of IT/OT Convergence: Design & Implementation Challenges [21]	Identify design/implementation issues and propose assessment tooling for IT/OT convergence.	References ISO/IEC 27030 (draft) and OCTAVE Allegro, maps to IEC/NIST concepts.	Governance: integration challenges between IT and OT teams; Risk: tool-based assessments for converged threats; Compliance: bridging audit evidence across domains; Performance: tool accuracy and automated metrics.
9	Industry 4.0 data security: A cybersecurity frameworks review [6]	Review applicability of GRC frameworks to Industry 4.0 data/security needs.	Compares ISO27001, IEC62443, NIST CSF and other frameworks.	Governance: need for governance layers that include OT stakeholders; Risk: highlights gaps for IIoT data flows; Compliance: recommends hybrid mappings; Performance: calls for domain-specific KPIs.
10	From COBIT to ISO 42001: Evaluating cybersecurity frameworks [14]	Comparative evaluation of major GRC frameworks for emerging tech readiness.	Directly compares COBIT, ISO/IEC 27001, NIST, ISO 42001, showing mapping opportunities.	Governance: recommends combining frameworks for board/management and operational needs; Risk: frameworks differ in coverage of new tech risks; Compliance: harmonisation required; Performance: proposes maturity/readiness indicators.
11	"I don't think we're there yet": Organisational learning from cyber incidents [10]	Qualitative study of post-incident learning practices.	Links incident metrics to organisational and regulatory reporting frameworks.	Governance: culture and learning critical to governance integration; Risk: repeated failure modes due to poor learning loops; Compliance: incident reporting quality affects compliance posture; Performance: emphasis on incident-to-learning KPIs (time-to-learn, corrective actions closed).
12	Winning the battle with cyber risk identification tools in ICS [22]	Empirical evaluation of cyber-risk identification tools for ICS.	Benchmarks tools against IEC 62443 technical/engineering controls.	Governance: tool selection is a governance decision; Risk: tool capabilities vary by OT constraints; Compliance: tools help evidence control implementation; Performance: measures tool accuracy, coverage and false-positive rates.

The thematic synthesis reveals several cross-cutting themes that directly support the four determinants of the proposed I-GRC Framework. Across the reviewed studies, governance integration emerges as a recurring challenge, with authors highlighting fragmented responsibility, limited board-level visibility, and inconsistent coordination between IT and OT teams. Similarly, risk management alignment is emphasized as essential, as many studies show that traditional IT-centric risk models fail to capture OT-specific constraints such as safety, availability, and real-time operation. The literature also underscores the importance of compliance harmonization, noting that existing standards—ISO/IEC 27001, ISA/IEC 62443, and NIST SP 800-82—are often applied in isolation, resulting in duplicated audits and misaligned control implementation. Finally, the reviewed research consistently stresses the need for performance measurement, particularly the use of maturity assessments, incident-based learning, and operational KPIs to evaluate cybersecurity effectiveness. Together, these themes confirm that a unified, measurable, and standards-aligned approach—such as the proposed I-GRC Framework—is needed to effectively manage IT-OT convergence in Saudi Arabia's critical sectors.

4.2. Analysis of ISO/IEC 27001

The ISO/IEC 27001 is the internationally accepted standard in determining, executing, upholding and constantly enhancing an Information Security Management System (ISMS). It offers a methodical way of dealing with the risk of information security by means of governance, risk evaluation, risk control and performance analysis. Although ISO/IEC 27001 has been extensively used in Information Technology environments, integrating it into Operational Technology (OT) systems is still difficult because the priorities of these two sets of technologies are different: IT is more concerned with confidentiality and integrity, whereas OT involves the consideration of availability and safety. Nevertheless, in the proposed Integrated IT-OT Governance, Risk, and Compliance (I-GRC) Framework, the ISO/IEC 27001 may be utilized as the governance foundation that will bring the two areas together under the umbrella security approach.

Regarding the integration of governance, ISO/IEC 27001 provides leadership responsibility, policy creation, and continuous improvement systems that may be applied to OT governance systems. Incorporating OT representation into the ISMS governance committee, organizations can make sure that both industrial control system (ICS) risks and corporate IT risks can be discussed, and the values of this approach are holistic decision-making.

To align risk management, the risk assessment process suggested in ISO/IEC 27001 (Clauses 6.1 and 8) can be adjusted to the characteristics of OT to cover OT-specific vulnerabilities, including device firmware and control system reliability. This, when coupled with ISA/IEC 62443 risk models, provides a way to consistently identify, assess and mitigate risks in both the IT and OT ecosystem.

With the compliance harmonization, the control goals of ISO/IEC 27001, espe-

cially the control objectives of Annex A, can be cross mapped with the requirements of IECs 62443-2-1 and NIST SP 800-82. This mapping will decrease the redundancy and make sure that compliance work towards the IT and OT will be unified into one audit and reporting framework (Figure 1).

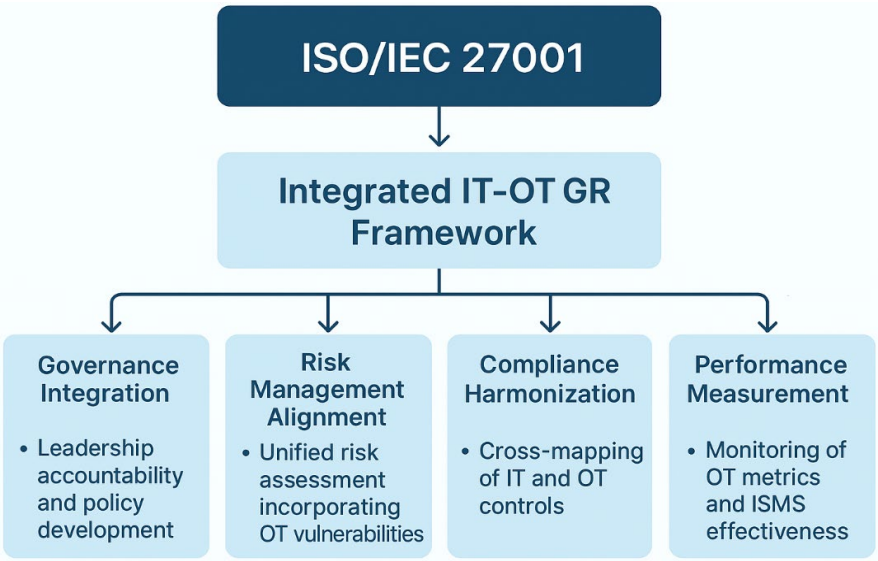

Figure 1. IT OT framework.

Lastly, performance measurement can be achieved through ISO/IEC 27001's continuous monitoring and internal audit requirements (Clause 9). By incorporating OT operational metrics—such as incident response time, system uptime, and control maturity level organizations can generate descriptive analytics that evaluate the overall performance of the unified I-GRC Framework, fostering evidence-based improvement and enhanced cybersecurity resilience.

4.3. Analysis of ISA/IEC 62443

The ISA/IEC 62443 series is a globally recognized framework for securing Industrial Automation and Control Systems (IACS). It offers a lifecycle-based and methodical approach to cybersecurity in Operational Technology (OT) settings. The framework is divided into various sections that deal with the organizational policies, system design, and technical controls. In the proposed Integrated IT Risk, Compliance and Governance (I-GRC) Framework, ISA/IEC 62443 is the OT equivalent of ISO/IEC 27001 that can offer domain-specific controls that may be integrated with enterprise governance and compliance processes.

Regarding the aspect of governance integration, the ISA/IEC 62443-2-1 (Security Program Requirements for IACS Asset Owners) and ISA/IEC 62443-2-4 (Requirements for Service Providers) focuses on the development of an organizational security program, role definition, and accountability. It is possible to reconcile these provisions with ISO/IEC 27001 Clause 5 (Leadership) to make sure that the IT and OT governance committees act within similar accountability

frameworks and have consolidated cybersecurity policies.

ISA/IEC 62443-3-2 (Security Risk Assessment and System Design) is similar to ISO/IEC 27001 (Clauses 6) (Planning and Risk Assessment) regarding alignment with risk management. It provides a systematic approach to defining zones, conduits, and critical assets, which are the main concepts of OT segmentation and network defense. By combining them, organizations can build a common risk register between IT and OT systems to integrate the digital and physical threat modeling.

For risk management alignment, ISA/IEC 62443-3-2 (Security Risk Assessment and System Design) aligns closely with ISO/IEC 27001 Clause 6 (Planning and Risk Assessment). It outlines a structured process for identifying zones, conduits, and critical assets—key concepts for OT segmentation and network defense. Integrating these methods allows organizations to create a shared risk register across IT and OT systems, combining digital and physical threat modeling.

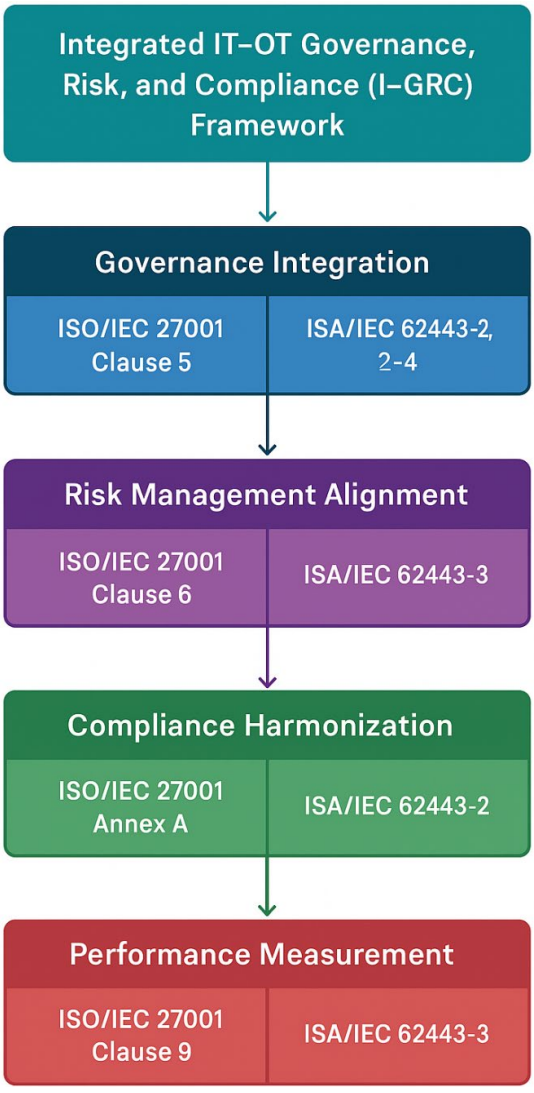

Figure 2. IT-OT GRC framework.

Under compliance harmonization, ISA/IEC 62443-4-2 (Technical Security Requirements for IACS Components) defines detailed control system-level security requirements, including authentication, data integrity, and use control (Figure 2). They can be cross mapped and the controls in the ISO/IEC 27001 Annex A made the process of auditing and reporting to be less tedious in both settings.

Lastly, the ISA/IEC 62443-2-3 (Patch Management for IACS) can serve as a driver of performance measurement by introducing such operational measures as patch compliance and patch response times. These indicators are used in conjunction with ISO/IEC 27001 Clause 9 (Performance Evaluation) when applied within an I-GRC framework to provide ongoing monitoring and improvement of entire integrated IT-OT cybersecurity areas, which increase resilience and regulatory compliance.

4.4. Analysis of NIST SP 800-82

NIST Special Publication (SP) 800-82 Revision 3, Guide to Operational Technology (OT) Security, is a comprehensive guideline that can be used to secure an Industrial Control system, Supervisory Control and Data Acquisition (SCADA) system, and Distributed Control System (DCS). It translates the principles of NIST Risk Management Framework (RMF) in NIST SP 800-37 and SP 800-53 to OT environments and links the IT security practices with the safety, reliability, and availability concerns of industrial systems. The NIST SP 800-82 is an operational interface that links the IT governance construct with OT-defined control implementation and monitoring in the context of the Integrated IT -OT Governance, Risk, and Compliance (I-GRC) Framework (Figure 3).

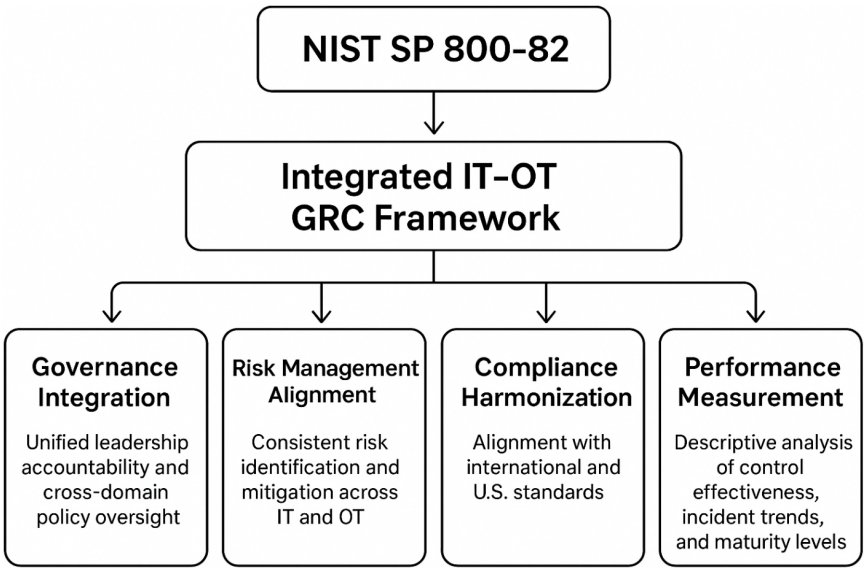

Figure 3. Integrated GRC framework.

Regarding the integration of governance, NIST SP 800-82, Section 3 defines control system owners, operations, and cybersecurity manager roles and respon-

sibilities. They can be aligned with ISO/IEC 27001 Clause 5 to create an integrated leadership responsibilities and cross-domain policy control.

To align risk management, Section 6 focuses on a six-step process of risk management RMF: categorize, selects, implements, assessing, authorizing, and monitor, which is the reflection of the ISO/IEC 27001 Clause 6 on planning and risk assessment. The ability to integrate this process into the I-GRC would allow risk detection and mitigation to be consistent over both IT and OT sectors.

In the compliance harmonization, Appendix G aligns OT security controls to NIST SP 800-53, which is used to base the alignment of U.S. federal and international standards (e.g., ISO/IEC 27001 and ISA/IEC 62443).

Lastly, the performance measurement is also in line with Section 7 of the NIST SP 800-82, which advises of constant monitoring and incident response measurements that are the main contributors to the performance dashboards of the I-GRC. These facilitate descriptive analysis of effectiveness of controls, trends of incidences, and level of maturity in integrated IT-OT ecosystems.

4.5. Proposed Framework

Based on above sections which include review of ISO/IEC 27001, ISA/IEC 62443, and NIST SP 800-82 standards and the review of 12 research articles and their proposed key themes, this research has proposed I-GRC framework for KSA. The I-GRC Framework provides a structured approach for unifying IT and OT cybersecurity governance, ensuring that both domains operate under a consistent risk and compliance model. It is designed to:

- Harmonize global standards such as ISO/IEC 27001, ISA/IEC 62443, and NIST SP 800-82
- Align with the National Cybersecurity Authority (NCA) guidelines of Saudi Arabia
- Enable measurement through descriptive indicators such as control maturity scores, incident frequency, and compliance alignment percentages

4.6. I-GRC Framework

The proposed I-GRC Framework:

- Bridges the gap between enterprise-level IT controls and industrial OT operations.
- Enables quantitative assessment using descriptive analytics for compliance maturity, risk reduction, and governance participation.
- Supports Saudi Arabia's Vision 2030 goals by strengthening national cybersecurity resilience and regulatory readiness.

4.7. Implementation Challenges

While the proposed I-GRC Framework offers a structured pathway for unifying IT and OT cybersecurity management, several practical challenges may arise during implementation. Organizational culture is often a significant barrier, as IT and

OT teams traditionally operate with different priorities, mindsets, and communication patterns, which can hinder cross-domain governance integration. Skill gaps also pose difficulties, particularly the shortage of professionals who possess combined IT-OT cybersecurity expertise and understand how international standards translate into industrial environments. Additionally, many critical infrastructure sectors rely on legacy OT systems that lack built-in security controls or cannot easily support modern monitoring, patching, or compliance mechanisms. These constraints may delay risk-alignment efforts or require costly upgrades. Finally, regulatory interpretation and resource allocation challenges—especially within organizations facing budget limitations or complex operational dependencies—can slow the harmonization of compliance processes. Recognizing these obstacles enables organizations to plan phased adoption strategies, capacity-building initiatives, and governance adjustments that support the effective and sustainable implementation of the I-GRC Framework (Figure 4).

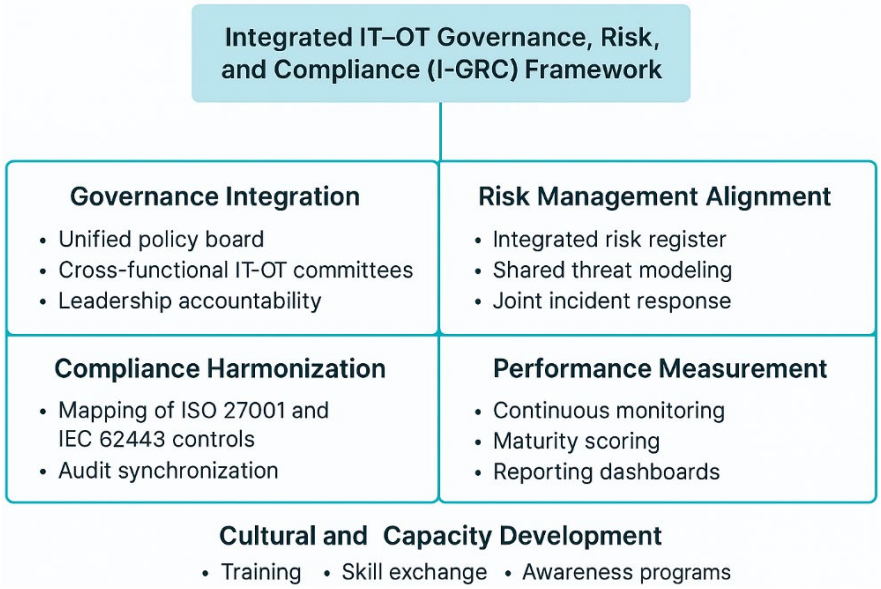

Figure 4. IT-OT, Risk compliance framework.

5. Conclusion and Future Research

5.1. Conclusion

The study has come up with an Integrated IT-OT Governance, risk and Compliance (I-GRC) Framework that is relevant to the cybersecurity and regulatory environment of the Kingdom of Saudi Arabia (KSA). The study revealed essential gaps and best practices to relate IT and OT cybersecurity management by conducting a thorough review of international standards ISO/IEC 27001, ISA/IEC 62443 and a meta-analysis of twelve studies that were published in 2020 and 2025 (CDS).

The suggested I-GRC Framework is a measurable, adaptive and structured model that helps to close the traditional gaps between the enterprise information

security and industrial operational safety. It simplifies the process of governance, coordinates risk management, reconciles the requirements across compliance, and provides performance measures in order to monitor and improve. The framework enables evidence-based decision-making focused on descriptive data analysis, increased visibility of cybersecurity performance, and the alignment with the international standards and with the recommendations of the National Cybersecurity Authority in Saudi Arabia (NCA).

In the end, the study will help to enhance the national cybersecurity stance and pursue the goals of the Vision 2030 of KSA by fostering a resilient, standardized, and data-driven model of IT-OT convergence management. I-GRC model is a viable guideline that policymakers, regulators and organizations aiming at the achievement of sustainable cyber resilience in a more interconnected digital ecosystem can use.

5.2. Future Research

Future research should empirically validate the proposed I-GRC Framework through case studies across Saudi Arabia's critical infrastructure sectors. Quantitative data collection on framework adoption, maturity assessment, and incident reduction metrics can strengthen its applicability, enabling continuous improvement, benchmarking, and adaptation to emerging technologies such as AI, IoT, and cloud-based OT systems.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] IBM (2024) Cost of a Data Breach Report 2024. IBM Security. https://www.ibm.com/reports/data-breach

[2] National Cybersecurity Authority (NCA) (2024) Annual Cybersecurity Report 2024. Government of Saudi Arabia.

[3] Kaspersky (2024) Industrial Cybersecurity Threat Landscape: Middle East Insights 2024. Kaspersky ICS CERT. https://ics-cert.kaspersky.com

[4] National Cybersecurity Authority (NCA) (2023) Essential Cybersecurity Controls (ECC-2). Government of Saudi Arabia. https://nca.gov.sa

[5] Maleh, Y. (2021) IT/OT Convergence and Cyber Security. *Computer Fraud & Security*, **2021**, 13-16.

[6] Toussaint, M., Krima, S. and Panetto, H. (2024) Industry 4.0 Data Security: A Cybersecurity Frameworks Review. *Journal of Industrial Information Integration*, **39**, Article 100604. https://doi.org/10.1016/j.jii.2024.100604

[7] Kiesow Cortez, E. and Dekker, M. (2022) A Corporate Governance Approach to Cybersecurity Risk Disclosure. *European Journal of Risk Regulation*, **13**, 443-463. https://doi.org/10.1017/err.2022.10

[8] Gale, M., Bongiovanni, I. and Slapnicar, S. (2022) Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead. *Computers & Security*, **121**, Article 102840. https://doi.org/10.1016/j.cose.2022.102840

[9] Slapničar, S., Axelsen, M., Bongiovanni, I. and Stockdale, D. (2023) A Pathway Model to Five Lines of Accountability in Cybersecurity Governance. *International Journal of Accounting Information Systems*, **51**, Article 100642. https://doi.org/10.1016/j.accinf.2023.100642

[10] Patterson, C.M., Nurse, J.R.C. and Franqueira, V.N.L. (2024) "I Don't Think We're There Yet": The Practices and Challenges of Organisational Learning from Cyber Security Incidents. *Computers & Security*, **139**, Article 103699. https://doi.org/10.1016/j.cose.2023.103699

[11] Boeding, M., Boswell, K., Hempel, M., Sharif, H., Lopez, J. and Perumalla, K. (2022) Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid. *Energies*, **15**, Article 8692.

[12] Racz, N., Weippl, E. and Seufert, A. (2010) A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In: De Decker, B. and Schaumül-ler-Bichl, I., Eds., *Communications and Multimedia Security*, Springer, 106-117. https://doi.org/10.1007/978-3-642-13241-4_11

[13] Schmitz, C., Schmid, M., Harborth, D. and Pape, S. (2021) Maturity Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners Assessment Capabilities. *Computers & Security*, **108**, Article 102306. https://doi.org/10.1016/j.cose.2021.102306

[14] McIntosh, T.R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., *et al.* (2024) From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models. *Computers & Security*, **144**, Article 103964. https://doi.org/10.1016/j.cose.2024.103964

[15] de Haes, S. and Van Grembergen, W. (2015) Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value. Springer.

[16] Humayed, A., Lin, J., Li, F. and Luo, B. (2017) Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, **4**, 1802-1831. https://doi.org/10.1109/jiot.2017.2703172

[17] Boyes, H., Hallaq, B., Cunningham, J. and Watson, T. (2018) The Industrial Internet of Things (IIoT): An Analysis Framework. *Computers in Industry*, **101**, 1-12. https://doi.org/10.1016/j.compind.2018.04.015

[18] Ehie, I.C. and Chilton, M.A. (2020) Understanding the Influence of IT/OT Convergence on the Adoption of Internet of Things (IoT) in Manufacturing Organizations: An Empirical Investigation. *Computers in Industry*, **115**, Article 103166. https://doi.org/10.1016/j.compind.2019.103166

[19] Yaacoub, J.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A. and Malli, M. (2020) Cyber-Physical Systems Security: Limitations, Issues and Future Trends. *Microprocessors and Microsystems*, **77**, Article 103201. https://doi.org/10.1016/j.micpro.2020.103201

[20] Dhirani, L.L., Armstrong, E. and Newe, T. (2021) Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors*, **21**, Article 3901. https://doi.org/10.3390/s21113901

[21] Zahran, B., Hussaini, A. and Ali-Gombe, A. (2023). IIoT-ARAS / Security of IT/OT convergence: Design and Implementation Challenges. arXiv.

[22] Rotibi, A., Saxena, N. and Burnap, P. (2024) Winning the Battle with Cyber Risk Identification Tools in Industrial Control Systems: A Review. *IET Cyber-Physical Systems: Theory & Applications*, **9**, 350-365. https://doi.org/10.1049/cps2.12105