MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

NATIONAL HIGHER SCHOOL OF MANAGEMENT

ENSM.KOLÉA.U.C

Thesis Submitted in Partial Fulfilment of the Requirements for

Master's Degree in «E-Government»

Leveraging Governance, Risk and Compliance GRC Frameworks to Enhance Technology Acceptance and Cyber Resilience in Digital Transformation Initiatives: Case study at the Directorate of Modernization -Ministry of Justice- Algeria

Elaborated by :

BOULALIAT Hadil

Supervised by:

Dr. BOUCHETARA Mehdi

Dr. MISSOUM Rafik

2024/2025

Abstract

This study explores how Governance, Risk, and Compliance (GRC) frameworks can serve as strategic enablers of digital transformation, addressing both human resistance and technical resilience. Using a qualitative methodology, including semi-structured interviews (human and AI experts) and a case study at Algeria's Ministry of Justice, the research highlights the critical interplay between formal governance structures and informal organizational dynamics. Findings reveal that effective GRC frameworks integrate policies with leadership influence, peer support, and cultural adaptation to enhance acceptance and cybersecurity. AI expertise contributed efficiency and standardization, while human insights ensured real-world adaptability, underscoring the power of hybrid intelligence. The study proposes reframing GRC from a control mechanism to a strategic capability, essential for cross-functional collaboration, adaptive risk management, and sustainable digital adoption. This contextualized approach is particularly vital for emerging economies, where global best practices must be tailored to local institutional realities.

Keywords: GRC, digital transformation, cybersecurity, hybrid intelligence, governance.

Résumé

Cette étude examine comment les cadres de Gouvernance, Risque et Conformité (GRC) peuvent agir comme leviers stratégiques de la transformation numérique, en traitant à la fois la résistance humaine et la résilience technique. À l'aide d'une méthodologie qualitative—comprenant des entretiens semi-structurés (experts humains et IA) et une étude de cas auprès du Ministère de la Justice algérien—la recherche met en lumière l'interaction cruciale entre les structures formelles de gouvernance et les dynamiques organisationnelles informelles. Les résultats montrent que des cadres GRC efficaces intègrent les politiques à l'influence managériale, au soutien entre pairs et à l'adaptation culturelle pour renforcer l'acceptation et la cybersécurité. L'expertise IA a apporté efficience et standardisation, tandis que les contributions humaines ont assuré l'adaptabilité opérationnelle, soulignant la valeur de l'intelligence hybride. L'étude propose de reconsidérer le GRC non plus comme un simple mécanisme de contrôle, mais comme une capacité stratégique, indispensable à la collaboration interfonctionnelle, à la gestion adaptative des risques et à l'adoption numérique durable. Cette approche contextualisée est particulièrement essentielle pour les économies émergentes, où les meilleures pratiques mondiales doivent être ajustées aux réalités institutionnelles locales.

Mots-clés : GRC, transformation numérique, cybersécurité, intelligence hybride, gouvernance.

الملخص

تستكشف هذه الدراسة كيف يمكن لأطر الحوكمة وإدارة المخاطر والامتثال أن تكون محفّزات استراتيجية للتحول الرقمي، من خلال التعامل مع مقاومة الأفراد والمخاطر التقنية معًا. باستخدام منهجية نوعية تشمل مقابلات شبه مُنظّمة (مع خبراء بشريين وذكاء اصطناعي) ودراسة حالة بوزارة العدل الجزائرية، تبرز الدراسة التفاعل الحيوي بين الهياكل الرسمية للحوكمة والديناميات التنظيمية غير الرسمية. تكشف النتائج أن الأطر الفعّالة توائم السياسات مع تأثير القيادة، ودعم الزملاء، والتكيف الثقافي لتعزيز القبول والأمن السيبراني. وأسهمت خبرة الذكاء الاصطناعي في تحقيق الكفاءة والتوحيد القياسي، بينما ضمنت الرؤى البشرية القابلية للتطبيق العملي، مما يبرهن على قوة الذكاء الهجين. وتقترح الدراسة إعادة صياغة مفهوم GRC من آلية رقابية إلى قدرة استراتيجية ضرورية للتعاون العابر للوظائف، وإدارة المخاطر التكيفية، واعتماد الرقمنة بشكل مستدام. وتكتسب هذه المنهجية السياقية أهمية خاصة للاقتصادات الناشئة، حيث يجب تكييف أفضل الممارسات العالمية مع الواقع المؤسسي المحلي.

الكلمات المفتاحية: GRC، التحول الرقمي، الأمن السيبراني، الذكاء الهجين، الحوكمة.

Acknowledgments

To my supervisors, MR.BOUCHETARA mehdi and MR.MISSOUM rafik, and my tutor, MR.MOUDJADJ Mustapha, thank you for your patience, wisdom, and unwavering support. Your guidance was more than just academic; it definitely shaped my thinking, helped me navigate challenges, and gave me the confidence to keep pushing forward even when the path wasn't clear.

To my dad, whose trust and belief carried me through every step, I wouldn't be here without you. To my mom, who did everything she could to encourage me, even when I doubted myself. To my brothers, who reminded me that I was never alone, who cared in ways that meant more than they know, I appreciate it beyond words.

To my friends, the ones who stayed close, through the late nights, the doubts, and the victories, you carried me when I couldn't carry myself. Your presence, patience, and belief in me made all the difference.

And to myself, thank you for staying, for showing up even when it hurt, for trusting the process when walking away felt easier.

This isn't just the end of a thesis. It's a soft, proud exhale. A reminder that I made it, and that I wasn't alone in getting here.

B,hadil

Summary

List of Tables

List of Figures

List of Symbols and Abbreviated Terms

ACADYC – Assessing Capability, Dynamics, and Change (Diagnostic Framework)

AI – Artificial Intelligence

CIA Triad – Confidentiality, Integrity, and Availability

COBIT – Control Objectives for Information and Related Technology

Cyber Resilience – Organizational ability to withstand cyber threats

DT – Digital Transformation

EGL – E-Government Literacy

GDPR – General Data Protection Regulation

GRC – Governance, Risk Management, and Compliance

ISO – International Organization for Standardization

ISO 22301 – Business Continuity Management Standard

ISO 27001 – Information Security Management Standard

IT – Information Technology

ITIL – Information Technology Infrastructure Library

KPI – Key Performance Indicator

ML – Machine Learning

NIS2 – Network and Information Security Directive 2

NIST – National Institute of Standards and Technology

OT – Operational Technology

PCI DSS – Payment Card Industry Data Security Standard

PSD2 – Payment Services Directive 2

RaaS – Ransomware-as-a-Service

RSSI – Responsable de la Sécurité des Systèmes d'Information (Information Security Officer)

SCADA – Supervisory Control and Data Acquisition

SIEM – Security Information and Event Management

SOC – Security Operations Center

SOX – Sarbanes-Oxley Act

TAM – Technology Acceptance Model

TC – Technological Capital

UNDESA – United Nations Department for Economic and Social Affairs

UTAUT – Unified Theory of Acceptance and Use of Technology

Introduction

In the contemporary global landscape, digital transformation (DT) has transcended buzzword status to become a fundamental imperative for organizational survival, competitiveness, and societal progress. Driven by rapid technological advancements, shifting market dynamics, and evolving citizen expectations, organizations across public and private sectors are compelled to reimagine their operations, value creation models, and stakeholder interactions through the lens of digital innovation (UNITED NATIONS DEPARTMENT FOR ECONOMIC AND SOCIAL AFFAIRS, 2024). This transformative wave promises unprecedented opportunities for efficiency, reach, and service enhancement. However, it simultaneously introduces significant complexities and challenges, encapsulated by the concept of "Digital Darwinism",the stark reality that failure to adapt digitally risks obsolescence (Rachmatika, 2019a); (Christie & Geary, 2024a), The journey of digital transformation is fraught with obstacles that span both human and technical domains. On the human front, organizations grapple with resistance to change stemming from disrupted routines and perceived threats, low levels of technology acceptance influenced by factors like perceived usefulness and ease of use, cultural inertia, and persistent skills gaps, particularly in cybersecurity (Rebecca Pariela & Suparno, 2024); (*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a); (Magsamen-Conrad et al., 2022). Trust in leadership and organizational processes emerges as a critical mediator in navigating these human-centric challenges (Doeze Jager et al., 2022).

Concurrently, the technical landscape presents formidable hurdles. Organizations face an exponentially expanding and increasingly sophisticated cyber threat environment, characterized by state-sponsored attacks, pervasive ransomware, Cybercrime-as-a-Service (CaaS), and AI-amplified threats targeting critical infrastructure and sensitive data (Canadian center for cybersecurity,2024, n.d.; *WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a). Ensuring the confidentiality, integrity, and availability (CIA triad) of systems while managing complex technological interdependencies and potential vulnerabilities inherent in co-evolving technologies (Altaleb & Rajnai, 2024); (Altaleb & Rajnai, 2024) demands robust technical controls and a proactive approach to cyber resilience.

Amidst these dual challenges, Governance, Risk, and Compliance (GRC) frameworks are often implemented primarily to ensure regulatory adherence and establish operational controls. While essential for maintaining order and accountability, the potential of GRC to serve a more strategic function, acting as an enabler rather than merely a constraint, remains significantly underexplored in the context of digital transformation. Existing literature often

treats GRC, change management, and cybersecurity as separate domains, overlooking the potential synergies and the role GRC could play in holistically addressing both the human and technical facets of transformation.

Research Problem and Questions

This thesis addresses the critical gap in understanding how GRC frameworks can be leveraged beyond compliance to strategically facilitate successful digital transformation. Specifically, it investigates GRC"s potential role in mediating the interplay between human challenges (resistance, acceptance, culture) and technical challenges (cyber threats, resilience). The central problem is the lack of in-depth insight into how GRC can function as a strategic bridge, enabling organizations to navigate the socio-technical complexities of digitalization more effectively.

To explore this problematic, the research is guided by the following main question:

1. **How can Governance, Risk, and Compliance (GRC) frameworks support organizations in addressing both human and technical challenges during digital transformation?**

This overarching question is further broken down into two sub-questions:

2. In what ways do GRC practices influence change management and reduce resistance to technology adoption among employees?
3. How do organizations use GRC to mitigate cyber threats and build cyber resilience during digital transformation initiatives?

Research Approach and Contribution

Adopting an interpretivist epistemology and employing a qualitative, exploratory research design, this study utilizes semi-structured interviews with both human experts and AI-simulated experts, alongside an embedded case study within a key public sector institution (Directorate of Modernization, Ministry of Justice, Algeria. Data analysis leverages the Gioia Methodology to systematically derive insights from participant perspectives.

This research aims to contribute a nuanced understanding of GRC"s strategic potential in digital transformation. By examining how GRC practices intersect with change management, technology acceptance, cybersecurity, and resilience, the study seeks to

provide actionable insights for organizations seeking to navigate their digital journeys more effectively. It challenges the conventional view of GRC as purely a control function, proposing instead a model where GRC acts as an integrated, strategic enabler that harmonizes human and technical imperatives for sustainable digital success.

Chapter 01: Theoretical Framework

As digital transformation accelerates, its success increasingly hinges on the governance structures that guide its execution. Scholars such as (Shahim et al., 2012) and (Coccia, 2019) argue that beyond deploying technologies, organizations must align institutional processes, risk thinking, and cultural adaptation to navigate today's complex digital environment. Governance, Risk, and Compliance (GRC) frameworks, traditionally seen as compliance tools, are now being reframed as strategic enablers that can bridge human-centered challenges and technical uncertainties.

This chapter lays the theoretical foundation for viewing GRC not as a rigid apparatus, but as a socio-technical system capable of integrating diverse transformation dimensions. Recent literature (Magsamen-Conrad et al., 2022); (Rachmatika, 2019b) emphasizes the critical role of trust, perception of risk, and institutional culture in shaping technology acceptance and organizational resilience, elements often neglected in rigid GRC deployments.

Accordingly, this chapter is structured into three analytical sections. The first addresses the role of GRC in managing human-centered challenges such as resistance to change and technology adoption. The second examines how GRC frameworks operationalize cybersecurity and cyber resilience. The third presents applied cases that highlight contextual variations in GRC implementation, especially in developing-country environments.

Together, these components construct a conceptual lens through which GRC is repositioned as a flexible, context-aware capability, essential for navigating the socio-technical dynamics of digital transformation.

Section 1: GRC and Human Centered Challenges in Digital Transformation

The human dimension of digital transformation is among the most significant challenges organizations face. Despite technological advances, successful adoption and integration depend heavily on factors such as organizational culture, employee acceptance, leadership trust, workforce agility, and addressing persistent cyber skills shortages (*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-b); (Magsamen-Conrad et al., 2022). (Christie & Geary, 2024b) emphasize cultivating a corporate culture that embraces change and challenges the status quo, while also recognizing the ethical complexities related to privacy, security, and algorithmic bias. For example, AI-enabled social engineering attacks like deepfake fraud highlight the intertwined human-technical risks (*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a).

Additional challenges include insufficient training (Arribi & Boutarfa, 2024), lack of expertise particularly in SMEs (Adedamola Oluokun, Adebimpe Bolatito Ige, et al., 2024), and resistant organizational cultures (Rebecca Pariela & Suparno, 2024). This section examines these human-centered issues and explores how strategically aligned Governance, Risk, and Compliance (GRC) principles (Shahim et al., 2012) can reshape perceptions and behaviors, enabling smoother and ethically responsible digital transformation.

(*WEF_Global_Cybersecurity_Outlook_2025*, n.d) presents a range of strategies organizations adopt to address the shortage of cybersecurity talent, each of which can be interpreted through the lens of Governance, Risk, and Compliance (GRC). The most dominant approach, cited by 76% of respondents, involves upskilling existing employees. This strategy reflects a strong governance commitment to long-term internal capacity-building and aligns with compliance objectives by ensuring that personnel meet evolving cybersecurity standards through structured, organization-led training. Recruiting experienced cyber professionals, chosen by 54% of organizations, indicates a governance-driven initiative aimed at quickly filling critical skill gaps, while simultaneously mitigating operational risk through external expertise acquisition. Meanwhile, promoting apprentice programmes (24%) also reflects a governance and compliance-oriented approach, supporting structured workforce development and adherence to national training standards.

Conversely, strategies such as expecting employees to independently upskill themselves (24%) suggest a shift of risk responsibility to individuals, highlighting a weaker governance structure and potentially inconsistent outcomes. Recruiting outside traditional cyber credentials (23%) represents a more risk-tolerant approach, favoring innovation and inclusivity but possibly introducing compliance challenges if professional standards are bypassed. Lastly, the 7% attributed to "Other" may indicate ad-hoc or reactive measures, underscoring the absence of a coherent GRC framework. Overall, this distribution of strategies reveals varying degrees of GRC maturity among organizations, with some favoring structured, policy-aligned approaches and others relying on fragmented or individual-driven solutions to bridge the cybersecurity skills gap.

Table 1: Strategic Responses to Cybersecurity Skills Gaps Mapped Against GRC Dimensions

Strategy	GRC Lens	Key Implications
Upskill our current employees	**Governance / Compliance**	Builds sustainable capability; aligns with internal policy.
Recruit experienced cyber professionals	**Governance / Risk**	Quick solution; mitigates immediate talent risk.
Promote apprentice programmes	**Governance / Compliance**	Long-term planning; supports compliance with talent policies.
Expect employees to independently upskill themselves	**Risk / Weak Governance**	Risk shifted to employees; may lack consistency.
Recruit outside traditional cyber credentials	**Risk / Compliance Risk**	Innovative but risks violating industry norms.
Other	**Unspecified**	Could imply reactive or unstructured practices.

Source: elaborated by the student inspired by (*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a)

Resistance to change is a natural human response and a key barrier to digital transformation (Rebecca Pariela & Suparno, 2024). The disruption of established routines inherent in DT often triggers such resistance. Hierarchical and resistant organizational cultures are frequently cited obstacles to effective GRC and digital transformation implementation ((Arribi & Boutarfa, 2024); (Rebecca Pariela & Suparno, 2024)). (Adebayo Adeyinka Victor et al., 2024)note that overlooking organizational culture remains a common failure point. Trust plays a critical role; empirical findings by (Doeze Jager et al., 2022) show an inverse relationship between organizational trust and resistance. Additional factors include low cybersecurity awareness in the general population (Vergara Cobos, 2024)and technical skill shortages, particularly in regions like Algeria (Arribi & Boutarfa, 2024). GRC frameworks contribute by promoting a security-conscious culture through training and communication (Adedamola Oluokun, Adebimpe Bolatito Ige, et al., 2024); (Benita Urhobo, 2024), alongside establishing clear digital governance policies that prioritize transparency and data protection (Arribi & Boutarfa, 2024)

Technology acceptance, distinct from mere usage or adoption, is crucial for successful digital transformation (Magsamen-Conrad et al., 2022). Foundational theories underpinning acceptance include the Theory of Reasoned Action (Fishbein & Ajzen, 1975), the Theory of Planned Behavior (Ajzen, 1985, 1991), and the Technology Acceptance Model (Davis, 1989), which emphasizes perceived usefulness and ease of use (Taherdoost, 2018)

(Magsamen-Conrad et al., 2022). The Unified Theory of Acceptance and Use of Technology (UTAUT) synthesizes eight models and incorporates factors such as performance expectancy, effort expectancy, social influence, and facilitating conditions. The same author note its relevance to health contexts and highlight the importance of integrating privacy and security concerns. (Rachmatika, 2019) identifies perceived digital risk as a key barrier to acceptance. Their "TAM-Governance Extension" model further advances this position by embedding GRC principles into acceptance mechanisms.

In the context of (Taherdoost, 2018) synthesized model of technology adoption and acceptance theories, a GRC-based reinterpretation reveals notable gaps and strengths. While early models such as TRA, TPB, and TAM emphasize user intention and perceived utility, they lack embedded mechanisms for governance alignment or regulatory compliance. More integrative frameworks like UTAUT and extensions such as Igbaria's Model or the TAM-Governance Extension begin to incorporate contextual variables such as institutional influence and trust, which are crucial for addressing digital risk and compliance. The following table maps each model to its potential contribution to Governance (e.g., leadership, institutional support), Risk Management (for example:addressing uncertainty, digital risk), and Compliance (for example: alignment with privacy and regulatory standards), thus offering a structured foundation for evaluating their utility in GRC-sensitive digital transformation efforts.

Table 2:GRC-Oriented Mapping of Technology Adoption and Acceptance Models (Adapted from Taherdoost, 2018)

Model	Governance	Risk Management	Compliance
Theory of Reasoned Action (TRA)	Weak: Individual-focused	Minimal: No risk constructs	Absent: No compliance reference
Theory of Planned Behavior (TPB)	Moderate: Includes perceived control	Limited: Suggests behavioral uncertainty	Absent
Technology Acceptance Model (TAM)	Weak: Emphasis on usability	Indirect: Perceived ease-of-use mitigates adoption risk	Not embedded
Social Cognitive Theory (SCT)	Moderate: Includes social influence	Moderate: Self-efficacy addresses perceived competence risk	Weak: No direct regulatory mapping
Diffusion of Innovations (DOI)	Weak: Innovation-focused, not policy-aligned	Partial: Considers innovation complexity	Not addressed

Model	Governance	Risk Management	Compliance
Motivational Model (MM)	Weak: Focused on intrinsic motivation	Weak: Ignores external threats	Absent
Uses and Gratification Theory (U&G)	Minimal: User-driven	Weak: Not risk-aware	Absent
Model of PC Utilization (MPCU)	Moderate: Facilitating conditions considered	Limited: Predictive of behavior, not risk	Absent
Theory of Interpersonal Behavior (TIB)	Moderate: Social and emotional norms involved	Limited: Suggests influence mechanisms	Weak
Igbaria's Model (IM)	Stronger: Includes job relevance, institutional factors	Moderate: Addresses external support	Partial: Usable in structured IT contexts
TAM Extension	Moderate: Broader context included	Limited: Still perception-based	Still not full compliance-oriented
UTAUT & Compatibility Models	Strong: Institutional context included	Emerging: Incorporates facilitating conditions	Potential: May support compliance via extensions

Source: elaborated by the student inspired by (Taherdoost, 2018)

Expanding adoption considerations to marginalized and underserved populations, (Magsamen-Conrad et al., 2022) introduce the concept of *"Technological Capital"* (TC). This concept moves beyond the traditional digital divide by encompassing awareness, knowledge, access, technological skills, and social support, all of which affect how individuals and groups engage with and adopt innovations. It shifts focus from labeling vulnerable groups toward addressing gaps in facilitating conditions and mitigating *"technological undercapitalization"* (Magsamen-Conrad et al., 2022). Governance, Risk, and Compliance (GRC) efforts that prioritize comprehensive training (Adedamola Oluokun, Courage Idemudia, et al., 2024) (Benita Urhobo, 2024), clear communication, and equitable resource allocation are instrumental in building organizational technological capital.

Within this context, (Rachmatika, 2019)TAM-Governance Extension model, illustrated in the "Digital Era Paradox" framework, provides a critical bridge between individual-level acceptance constructs and systemic GRC structures. It integrates classical acceptance factors (for example: perceived risk, trust belief, behavioral intention) with institutional enablers such as IT GRC, customer due diligence, access control, and monitoring. These governance levers reinforce structural assurance, reduce perceived risk, and increase trust belief, which collectively shape the behavioral intention to use. Such mechanisms align with (Doeze Jager

et al., 2022), who highlight trust as central to digital adoption, and with the (UNITED NATIONS, 2024) emphasis on "inclusion by design." Notably, the model demonstrates how GRC dimensions not only regulate systems but enable digital inclusion by reducing psychological barriers and building technological capital—especially among digitally underserved groups.

The table below summarizes the key components of the TAM-Governance Extension model and maps them to their respective Governance, Risk, and Compliance (GRC) functions, highlighting their role in promoting digital trust and inclusion,(Rachmatika, 2019).

Table 3: GRC-Based Mapping of the TAM-Governance Extension Model

Model Element	GRC Dimension	Function in Model	Contribution to Digital Inclusion / Trust
IT GRC	Governance	Provides institutional structure for monitoring, compliance, and access control	Builds systemic trust; ensures oversight and accountability
Customer Due Diligence	Compliance	Verifies user identity and legitimacy, especially in sensitive sectors (e.g., finance, health)	Reduces uncertainty and fraud risk; increases confidence among marginalized users
Access Control	Governance/Risk	Limits exposure to unauthorized users; enforces role-based permissions	Prevents breaches and protects user data; essential for trust and perceived fairness
Monitoring	Governance/Risk	Ensures ongoing system integrity and detects anomalies in behavior or access	Supports reliability and transparency of systems
Structural Assurance	Governance	Combines policies, certifications, and guarantees to ensure system dependability	Bridges the gap between institutional credibility and user perception
Perceived Risk	Risk Management	Cognitive evaluation of uncertainty, often mitigated through trust mechanisms	Lower risk perception is essential for adoption in low-literacy or high-risk communities
Trust Belief	Governance/Risk	Influenced by structural assurance and past experience; boosts behavioral intention	Central to adoption among vulnerable or skeptical populations
Self-Efficacy	Governance (indirect)	User's confidence in using technology;	Boosted by inclusive training strategies (aligned with GRC

Model Element	GRC Dimension	Function in Model	Contribution to Digital Inclusion / Trust
		influenced by training and usability design	capacity-building practices)
Behavioral Intention to Use	Outcome (Governance-enabled)	Final construct influenced by risk, trust, and systemic assurances	Reflects successful alignment of user perception with organizational trust infrastructure

Source: elaborated by the student inspired by (Rachmatika, 2019b)

Building on the notion of *Technological Capital* (Magsamen-Conrad et al., 2022), which frames digital engagement as a function of skills, access, and social support rather than merely infrastructure, recent international efforts have emphasized the importance of operationalizing this concept within governance frameworks. (UNITED NATIONS 2024, 2024) introduces "*e-government literacy" (EGL)* as a key sub-index of the Human Capital Index (HCI) in its latest E-Government Survey. EGL assesses the ability of all population segments ,particularly vulnerable groups, to fully leverage e-government services and participate in digital civic life. Importantly, while many digital maturity frameworks concentrate on supply-side infrastructure, EGL highlights the need to address demand-side gaps through a combination of "push" (e.g., training, infrastructure access) and "pull" (e.g., trust, usability) factors. This aligns with GRC-based strategies that emphasize inclusive governance, citizen data protection, risk reduction through digital education, and institutional accountability.

The table below maps the core components of e-government literacy to the Governance, Risk, and Compliance (GRC) framework, illustrating how EGL functions as both a measurement tool and an operational entry point for building digital inclusion.

Table 4: Mapping E-Government Literacy (UN, 2024) to GRC Dimensions and Technological Capital

EGL Dimension	GRC Domain	Strategic Role	Contribution to Technological Capital
Awareness of Services	Governance	Public communication, outreach, and policy framing	Builds recognition of access rights and participation opportunities
Digital Knowledge and Skills	Risk / Governance	Training programs to reduce user error and increase capability	Enhances confidence and usability among low-

EGL Dimension	GRC Domain	Strategic Role	Contribution to Technological Capital
			digital-literacy populations
Equitable Access to Digital Infrastructure	Governance / Compliance	Ensures inclusive service delivery aligned with legal access mandates	Reduces infrastructural exclusion and systemic marginalization
User Data Protection	Compliance	Enforces privacy laws, transparency in use, and access control	Increases trust and perception of security in digital systems
Civic Participation Enablement	Governance	Supports democratic digital participation channels (e-consultation, feedback)	Empowers citizens, especially the underserved, to co-shape digital governance
Support Services / Digital Helpdesks	Risk Management	Risk mitigation via user assistance and technical support	Prevents drop-off in usage due to confusion or technical barriers

Source: elaborated by the student inspired by (UNITED NATIONS 2024, 2024)

Synthesis

Governance, Risk, and Compliance (GRC) frameworks can reshape organizational perceptions and behaviors to facilitate smoother digital transformation. By fostering trust and establishing transparent processes, GRC reduces ambiguity through clearly defined roles (Adebayo Adeyinka Victor et al., 2024) and emphasizes accountability and ethical conduct (*A Process Model for Integrated IT Governance, Risk, and Compliance Management*, n.d.).; (Siahaan et al., 2023); (McIntosh et al., 2023), addressing ethical concerns highlighted by (Christie & Geary, 2024)and strengthening trust (Doeze Jager et al., 2022). IT GRC specifically mitigates perceived digital risks by enhancing structural assurance mechanisms such as access control, customer due diligence, and system monitoring (Rachmatika, 2019b). Furthermore, GRC promotes principles such as inclusion by design and digital literacy (UNITED NATIONS 2024, 2024), including push-and-pull strategies to foster demand-side readiness. It supports bridging skills gaps (Adedamola Oluokun, Adebimpe Bolatito Ige, et al., 2024; Arribi & Boutarfa, 2024; *WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a) and actively builds organizational technological capital by improving awareness, knowledge, access, and capabilities (Magsamen-Conrad et al., 2022). Integrating user acceptance theories into GRC initiatives (Magsamen-Conrad et al., 2022; Rachmatika, 2019b; Taherdoost, 2018) and aligning these efforts strategically with people and processes (Shahim

et al., 2012)reduces adoption barriers and cultivates a more receptive, skilled, and agile workforce.

Section 2: GRC and Technical Challenges – Cybersecurity and Resilience

As organizations accelerate digital transformation, they face an increasingly complex cybersecurity environment defined by rapidly evolving threats, interdependent systems, and infrastructure disparities. The Canadian Centre for Cyber Security (Canadian center for cybersecurity,2024, n.d.)

and World Economic Forum (*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a)warn of intensifying threat complexity, citing advanced state-sponsored campaigns by actors such as China, Russia, and Iran targeting critical infrastructure. Simultaneously, ransomware remains a prevalent attack vector—especially affecting small and medium enterprises (SMEs) and essential sectors—compounded by the rise of Cybercrime-as-a-Service (CaaS), which lowers entry barriers for threat actors (Adedamola Oluokun, Courage Idemudia, et al., 2024). These developments expose not only technological gaps but strategic governance deficiencies.

Technical sophistication further challenges resilience. Threat actors now deploy advanced tactics such as obfuscation, “big game hunting”, and “living off the land” methods, targeting edge devices and exploiting trusted systems ((Canadian center for cybersecurity,2024, n.d.) Adding to this complexity is the emergence of the AI–cyber paradox: while artificial intelligence (AI) is increasingly used to support security, it is also weaponized by adversaries to amplify attack impact, including through generative AI (*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a). Alarmingly, many organizations acknowledge AI threats but lack mature mechanisms for risk assessment and mitigation, thereby deepening systemic vulnerabilities.

According to (Coccia, 2019) theory of technological co-evolution, modern infrastructure introduces “parasitic” components,such as insecure IoT devices,that compromise “host” systems, dramatically expanding the attack surface. Supply chain interdependencies and vendor concentration exacerbate this exposure, especially in developing nations such as Algeria, where digital infrastructure remains underdeveloped (Arribi & Boutarfa, 2024). These multifaceted risks call for a strategic response,one that moves beyond reactive security postures toward integrated GRC frameworks capable of systematically assessing, governing, and reducing threat exposure while strengthening organizational resilience.

Governance, Risk, and Compliance (GRC) frameworks respond to these challenges by aligning cybersecurity with broader organizational goals. National Cybersecurity Strategies

(*Sereir El Hirtsi Hayet,2023*) emphasize principles like privacy, rule of law, and stakeholder collaboration, while also encouraging cross-sector resilience. Strategic GRC implementation, particularly when embedded into the architecture of public institutions and SME ecosystems, enables organizations to confront systemic threats through structured assessments, continuous monitoring, and policy alignment. This includes the adoption of risk-based insurance mechanisms, strengthening accountability and recovery preparedness for high-risk sectors.

The table below summarizes how GRC principles can be applied to address core complexity-driven vulnerabilities in today's cybersecurity landscape.

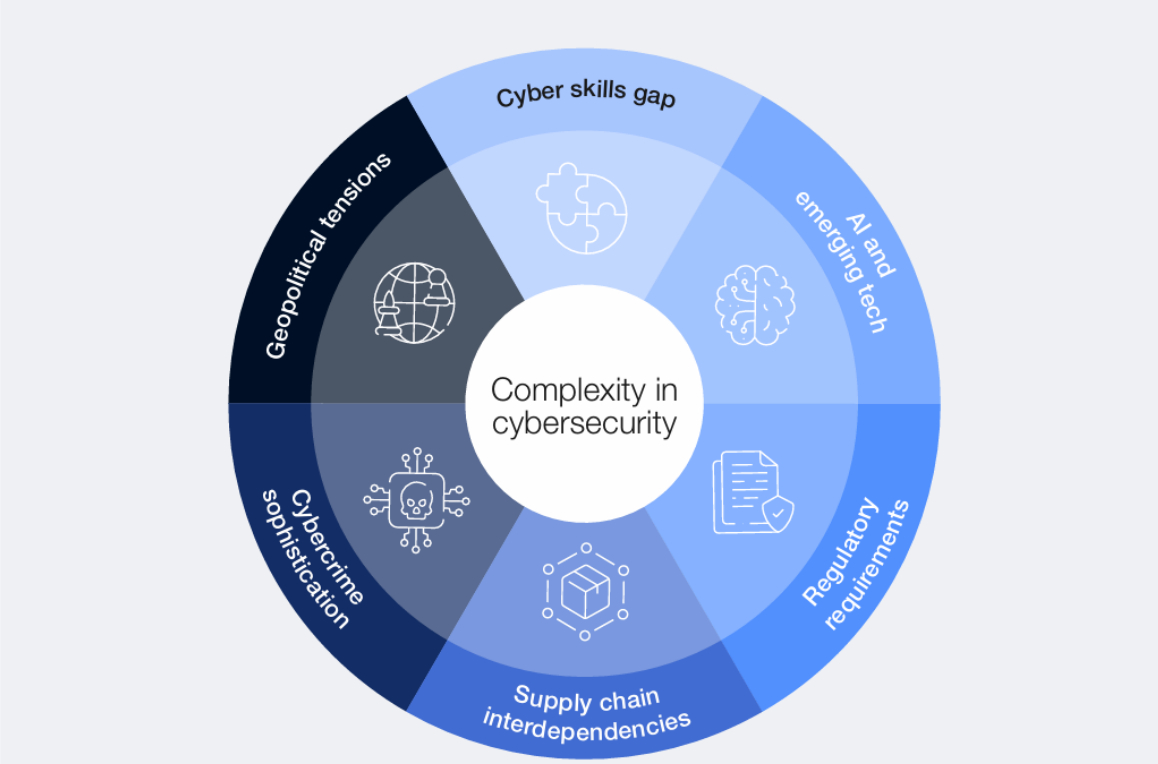
Table 5: Addressing Cybersecurity Complexity through GRC Frameworks

Complexity Source	GRC Dimension	Strategic GRC Role	Resilience Impact
Ransomware & Cybercrime-as-a-Service (CaaS)	Risk	Threat modeling, automated detection rules, internal audit controls	Reduces attack surface; prepares response protocols
AI-Generated Threats (AI-cyber paradox)	Governance/Risk	AI-specific risk assessments, ethical governance policies, AI incident simulation	Anticipates emerging risks; mitigates misuse of autonomous systems
Supply Chain Dependencies	Compliance/Risk	Third-party risk assessments, vendor certification frameworks (e.g., ISO 27001, NIST)	Limits exposure to external failures; enhances trust boundaries
Infrastructure Gaps in Developing Nations	Governance	Public–private partnerships, capacity-building programs, and national policy implementation	Builds foundational resilience; bridges the technological divide
IoT & Technological Co-Evolution (Coccia, 2018)	Governance/Risk	Asset inventorying, Zero Trust Architecture, segmentation policies	Prevents parasitic lateral movement across systems
Regulatory Fragmentation	Compliance	Harmonization with international standards (GDPR, ISO, NIST); compliance automation via AI	Prevents fatigue, ensures alignment, supports global resilience posture

Source: elaborated by the student

As digital systems become more embedded in organizational operations, cybersecurity evolves from a technical concern to a strategic and structural one.

Figure 1 : WEF (2025), "Global Cybersecurity Outlook 2025,"



Source: (*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a)

figure one illustrates six interconnected forces that amplify the complexity of cybersecurity: the cyber skills gap, the evolution of artificial intelligence, expanding regulatory requirements, supply chain interdependencies, increasingly sophisticated cybercrime tactics, and heightened geopolitical tensions. These factors do not operate in isolation but reinforce each other, creating a dense web of vulnerabilities that overwhelm conventional security approaches. For instance, AI accelerates both defense and attack capabilities, supply chain attacks exploit third-party relationships, and geopolitical actors integrate cyber operations into strategic conflict.

For organizations, this compounded complexity means that mitigation requires more than isolated controls—it requires a coordinated framework that integrates governance oversight, risk intelligence, and compliance alignment. GRC frameworks serve this role by structuring how threats are assessed, controls are prioritized, and responsibilities are assigned. By embedding security policies into governance, GRC ensures executive accountability. Through continuous risk assessment and scenario modeling, it enhances preparedness. Compliance mechanisms aligned with evolving regulations ensure that organizations do not fall behind legally or ethically. The result is a system-wide approach to resilience that responds to complexity with strategic structure, not fragmentation.

The table below maps the six complexity factors from Figure 1 to core GRC functions and illustrates how each element of GRC contributes to cyber resilience.

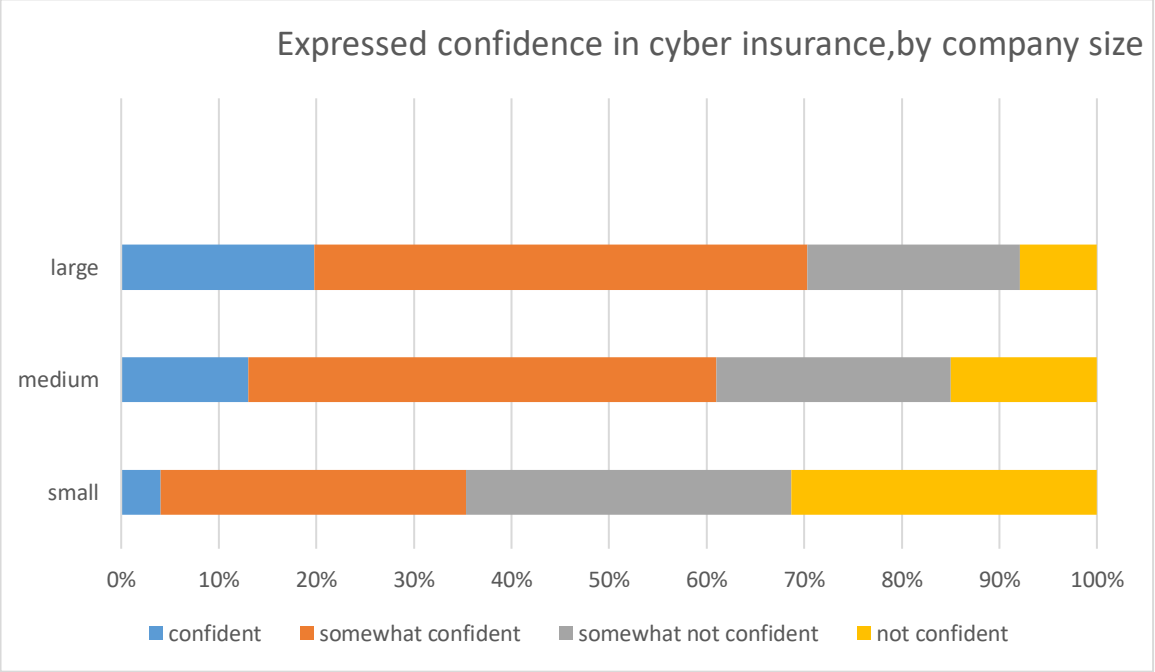
Table 6: Mapping Cybersecurity Complexity Factors to GRC Functions and Resilience Outcomes

Complexity Factor	GRC Domain	Strategic Role of GRC	Resilience Contribution
Cyber Skills Gap	Governance	Invest in structured training, security awareness programs, and role-based access	Reduces human error; builds operational preparedness
AI & Emerging Technologies	Risk / Governance	Conduct AI risk mapping, ethical governance, AI-use policies	Anticipates misuse; enables rapid detection of AI-driven threats
Regulatory Requirements	Compliance	Regulatory monitoring, automated compliance updates, integrated legal frameworks	Ensures continuity amid shifting legal expectations
Supply Chain Interdependencies	Risk / Compliance	Third-party audits, contractual clauses, vendor certifications	Isolates external risk; enables layered defense across partners
Cybercrime Sophistication	Risk	Threat modeling, anomaly detection systems, insider risk programs	Detects complex threat patterns before damage escalates
Geopolitical Tensions	Governance / Risk	Strategic scenario planning, threat intel integration, geopolitical risk registers	Enables proactive defense posture; avoids blind spots

Source: elaborated by the student inspired by(*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a)

While the multifaceted nature of cyber threats demands enterprise-wide structural responses, organizational capacity to absorb and manage such risks varies widel as illustrated in figure 2

Figure 2:Expressed confidence in cyber insurance,by company size



Source: (*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-b)

smaller organizations exhibit significantly lower confidence in their cyber insurance coverage compared to larger entities. This gap reveals a troubling vulnerability in resilience planning: although cyber insurance is not a replacement for security controls, it is a key instrument in risk transfer, incident response, and business continuity,all essential pillars of cyber resilience.

This disparity reflects broader governance and capability gaps. SMEs often lack the internal expertise, compliance resources, and formalized GRC structures that larger organizations leverage to negotiate adequate coverage and implement necessary controls. From a GRC perspective, this exposes weaknesses in risk governance maturity. Without proper risk classification, documentation, and mitigation strategies, insurance becomes costlier or even inaccessible, especially as underwriters grow more selective in the wake of surging ransomware claims.

GRC frameworks help level the playing field. Through structured risk assessments, compliance tracking, and formal governance protocols, organizations, regardless of size, can systematically demonstrate preparedness, lower risk exposure, and justify more favorable

insurance terms. In doing so, GRC becomes not only a security enabler but a financial resilience tool, especially for resource-constrained sectors.

The following table outlines how GRC practices influence cyber insurance readiness and contribute to resilience, particularly among under-resourced organizations.

Table 7 : Cyber Insurance Confidence by Organization Size

Barrier to Confidence	GRC Domain	GRC Action or Capability	Resilience Outcome
Limited awareness of policy requirements	Governance	Integrate cyber insurance literacy into security governance policies	Empowers informed risk transfer decisions
Inability to quantify or document risk	Risk	Implement formal risk registers, threat modeling, and impact analysis	Enables evidence-based negotiations with insurers
Lack of formal compliance controls	Compliance	Ensure baseline control coverage (e.g., NIST, ISO 27001)	Demonstrates due diligence, increases insurer confidence
Absence of incident response documentation	Governance / Risk	Create tested playbooks and disaster recovery plans	Reduces expected damage; qualifies for lower premiums
SME-specific resource constraints	Governance	Apply scalable GRC models with automated tracking and low-cost auditing	Makes resilience planning accessible without overburdening small teams

Source: elaborated by the student inspired by(*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a)

The digital divide is not merely a question of connectivity, but of functional access, readiness, and risk governance. As shown in (Adedamola Oluokun, Courage Idemudia, et al., 2024)SMEs face disproportionate barriers to digital access, including high costs, low awareness, lack of trust in digital systems, insufficient digital skills, and limited infrastructure. These constraints not only hinder participation in the digital economy but also weaken cyber resilience by leaving these organizations unprepared and exposed to increasingly complex and targeted cyber threats.

GRC frameworks, when appropriately adapted to the SME context, serve as practical mechanisms to overcome these barriers. From a governance perspective, they promote

leadership accountability in digital planning and investment. In terms of risk management, they help SMEs identify critical exposure points, even with minimal IT expertise, by offering simplified templates for threat assessment, backup planning, and supplier due diligence. From a compliance standpoint, GRC frameworks also assist in aligning SMEs with regulatory mandates (e.g., GDPR, PSD2) which increasingly apply regardless of organization size.

By embedding such frameworks in SME ecosystems, via national cybersecurity strategies, sector-specific standards, or SME consortia, governments and industry bodies can reduce systemic vulnerabilities, increase SME participation in secure digital ecosystems, and strengthen national cyber resilience overall. GRC in this context is not about formal bureaucracy, but about creating scalable and accessible pathways for risk-aware digital engagement.

The table below highlights how specific SME digital access barriers can be addressed through targeted GRC adaptations to build baseline cyber resilience.

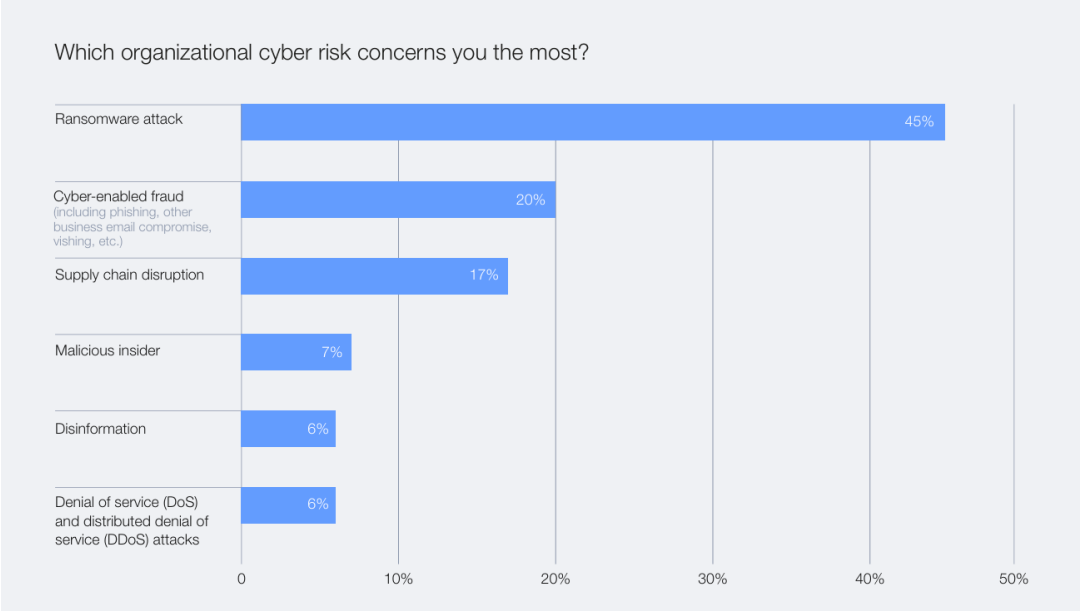
Table 8 :GRC-Oriented Solutions to Digital Access Barriers in SMEs

Barrier	GRC Domain	GRC-Based Intervention	Resilience Contribution
High Cost of Adoption	Governance	Promote subsidized national GRC schemes; sector-based shared services	Reduces entry cost for cybersecurity participation
Lack of Awareness	Governance	SME-targeted awareness campaigns, executive risk briefings	Builds risk ownership and strategic visibility
Low Digital Skills	Risk / Governance	Modular GRC onboarding, role-based risk tools	Enables contextual security practices without technical overload
Lack of Trust in Digital Tools	Compliance / Risk	Embed privacy-by-design, vendor due diligence templates	Increases confidence in tool adoption and reduces third-party risk
Limited Infrastructure & Support	Governance / Compliance	Regional cybersecurity hubs; minimum viable control packages	Bridges infrastructure gap while maintaining regulatory alignment

Source: elaborated by the student inspired by(Adedamola Oluokun, Courage Idemudia, et al., 2024)

As cyber threats become more advanced, strategic GRC implementation must move beyond checklists and reactive compliance.

Figure 3 :Organizational cyber risks ranked – 2025

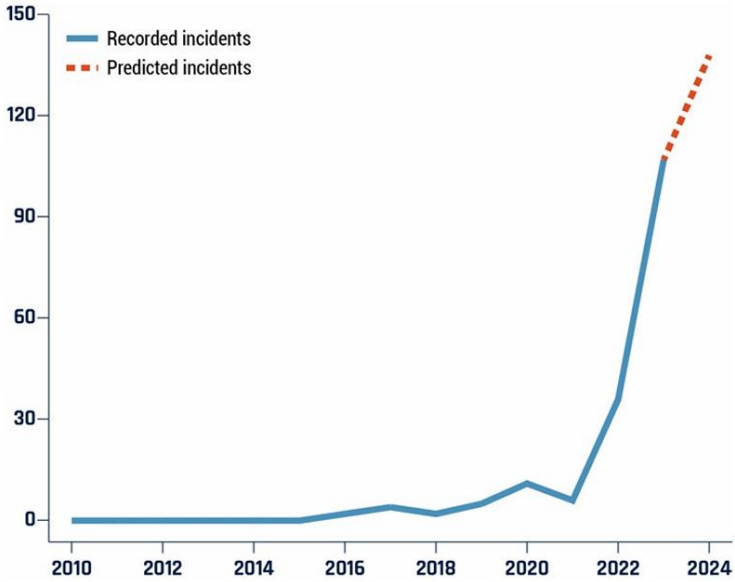


Source:(*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-a)

Figure 3, highlights that ransomware now ranks as one of the top cyber risks faced by organizations, surpassing traditional threats like insider attacks or data breaches. This is reinforced by (Canadian center for cybersecurity,2024, n.d.), which implied a steep increase in ransomware incidents, particularly in critical Canadian sectors. Attackers now deploy advanced techniques ,including obfuscation, lateral movement, and polymorphic malware, hat bypass conventional perimeter defenses.

The emergence of Ransomware-as-a-Service (RaaS), exemplifies the industrialization of cybercrime. These modular ecosystems allow less-skilled actors to launch sophisticated attacks by purchasing ransomware kits, hosting services, and even customer support. Compounding this threat environment, figure 4 shows the rise in publicly reported incidents involving AI-generated attacks, where synthetic phishing, deepfake content, and adaptive malware increase both deception and scale.

Figure 4 : Generative AI incidents



Source:(Canadian center for cybersecurity,2024, n.d.)

In response to these multi-vector threats, GRC frameworks provide the structural scaffolding for cyber resilience. Governance elements enable organizations to implement coherent security policies, clarify roles, and ensure escalation protocols are in place. Risk management processes integrate threat intelligence, penetration testing, and continuous monitoring. Compliance ensures that security actions align with legal obligations and stakeholder expectations, critical in sectors handling sensitive data.

Critically, as mentioned by (Benita Urhobo, 2024) , GRC capabilities are increasingly augmented by AI-driven systems that support automated compliance, real-time anomaly detection, and predictive threat modeling. These tools elevate GRC from a documentation exercise to a strategic platformenha, ncing not only defense but learning, speed, and foresight.

Table 9: GRC Framework Responses to Advanced Cyber Threat Ecosystems

Threat Feature	GRC Domain	Strategic GRC Response	Resilience Outcome
Surging Ransomware Attacks	Risk / Governance	Scenario planning, incident response playbooks, backup validation protocols	Faster containment and recovery
Use of Obfuscation Techniques	Risk / Compliance	Threat intelligence integration, sandboxing, multi-factor logging	Earlier detection of stealthy threats
Ransomware-as-a-Service Ecosystem	Governance	Attribution modeling, vendor behavior monitoring, third-party legal clauses	Better preparedness for supply chain exposure
AI-Powered Threats (Mutation, Phishing)	Governance / Risk	AI-threat simulation exercises, SOC behavior baselines	Dynamic defense posture; recognition of non-obvious threat patterns
Lack of Real-Time Response Capability	Compliance / Risk	Deployment of AI-driven GRC tools (alerts, auto-remediation, audit trails)	Enables continuous compliance and zero-delay threat response
Growing Regulatory Demands on Response Time	Compliance / Governance	Automate control reporting and evidence generation	Reduces compliance burden and increases legal defensibility

Source: elaborated by the student inspired by(Canadian center for cybersecurity,2024, n.d.)

In today's volatile cyber landscape, GRC frameworks no longer serve as passive compliance checklists, they are redefined as strategic infrastructure for building resilience and ensuring institutional adaptability. This strategic reorientation is captured in layered conceptual models that illustrate how governance, risk, and compliance span from high-level strategy to operational enforcement. These frameworks typically unfold in phases, starting with environmental analysis, moving through planning and execution, and culminating in embedded monitoring and enforcement mechanisms (Canadian center for cybersecurity,2024, n.d.) Interpreted through a GRC lens, governance ensures executive alignment and stakeholder clarity; risk management anchors predictive assessments and adaptive controls; and compliance sustains regulatory and ethical accountability across all digital transformation stages.

However, idealized models often meet friction in reality. Structural assessments show how barriers such as financial limitations, low cyber literacy, and fragmented legal environments can stall GRC execution, particularly within small and medium enterprises and digitally

underdeveloped sectors (Vergara Cobos, 2024). These barriers, when reframed through GRC, point to insufficient governance leadership, reactive rather than proactive risk frameworks, and a regulatory burden that discourages rather than enables security adoption.

The synthesis of these insights reveals a deeper truth: cyber resilience is not merely a function of technological robustness but of institutional capacity. When GRC is understood and implemented as a cross-cutting capability, defining leadership roles, structuring operational behaviors, and embedding learning cycles,it becomes the connective tissue that enables both stability and recovery. Instead of being a barrier, cybersecurity becomes a lever for strategic agility, enabling organizations to operate confidently amid disruption

The table below synthesizes how GRC frameworks can help organizations manage their exposure to complex cyber threat ecosystems, especially under geopolitical pressure.

Table 10: GRC Strategies for Exposure Management in Global Cyber Threat Ecosystems

Threat Vector / Ecosystem	GRC Domain	Strategic GRC Action	Resilience Outcome
State-Sponsored Threat Programs	Governance / Risk	Geopolitical risk registers, national threat modeling, government liaison roles	Enhances proactive readiness against advanced persistent threats
Industry-Specific Targeting (PRC policy focus)	Governance / Compliance	Sector-specific standards (e.g., IEC 62443 for ICS), export control compliance	Aligns defense posture with sector risk and regulatory regimes
Non-State Cybercrime Drivers	Governance / Risk	Sociopolitical context mapping, cybercrime heatmapping in supply chain zones	Anticipates weak links in governance exposure across ecosystems
Predicted Technical Vulnerabilities (2025)	Risk / Compliance	Cloud config audits, remote access reviews, software supply chain vetting	Closes known exposure points; improves vendor selection and oversight
Geopolitical Tensions & Strategic Realignment	Governance / Compliance	Scenario planning, jurisdictional data mapping, zero-trust investments	Aligns resilience strategy with global instability and fragmentation

Source: elaborated by the student inspired by the the review

While GRC is often perceived as a compliance instrument, the remaining figures introduce a more operational and systemic view, where GRC maturity and capability mapping become strategic tools for organizational transformation. One diagram outlines a multi-stage GRC maturity model, moving from reactive and fragmented compliance efforts toward optimized, proactive, and integrated practices across governance, risk, and compliance domains. Through the GRC lens, this progression reflects increasing levels of strategic alignment, automation, stakeholder integration, and resilience embedding.

In parallel, the strategic roadmap for GRC development illustrates a phased implementation sequence that prioritizes leadership buy-in, resource planning, capability building, and iterative feedback loops. It highlights how organizations can institutionalize GRC not just as documentation, but as a living system that evolves alongside digital transformation demands. Each phase of the roadmap introduces tools and processes that support measurable advancement, metrics, training, audits, and governance councils, essential for embedding GRC into the organizational fabric.

Finally, the GRC ecosystem layout model presents a holistic view of how various organizational functions, legal, IT, security, operations, audit, interconnect under a unified GRC framework. It highlights the structural interdependencies necessary for a successful GRC implementation, emphasizing the importance of cross-functional alignment, information sharing, and centralized oversight mechanisms. Through a GRC lens, this model calls for breaking down silos, building trust across teams, and enabling real-time risk visibility.

Together, these models transform GRC from a static policy toolkit into a dynamic capability-building infrastructure, one that fosters both compliance and innovation, enhances decision-making, and prepares the organization for evolving risk landscapes.

The table below summarizes how GRC maturity, structured development, and organizational alignment translate into enhanced capability, resilience, and agility.

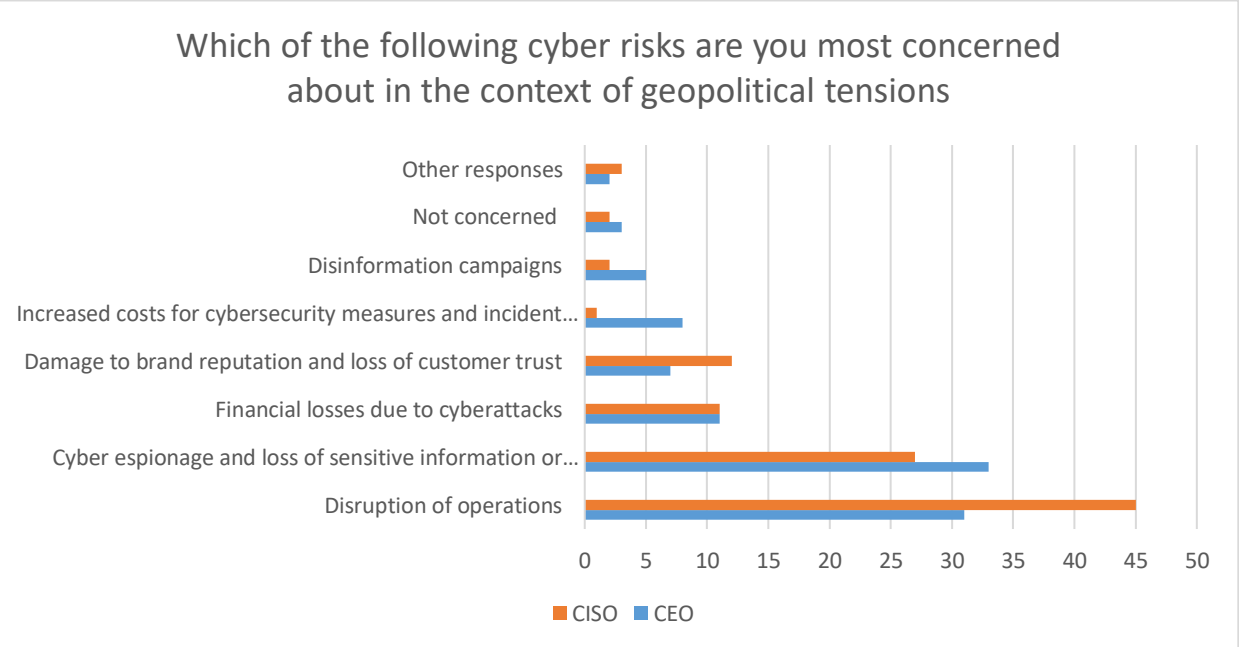
Table 11: GRC Analytical Table – Operationalizing GRC through Capability Models

Operational Focus	GRC Domain	Strategic GRC Action	Transformation Outcome
GRC Maturity Levels	Governance / Risk	Maturity assessments, KPI tracking, benchmarking	Institutionalizes progress tracking and drives strategic alignment
Capability Roadmap	Governance / Compliance	Phase-based implementation, leadership onboarding, feedback loops	Ensures sustainable, scalable adoption of GRC initiatives
Cross-functional GRC Ecosystem	Governance / Risk	Role clarity, central data hubs, multi-stakeholder integration	Breaks silos, builds trust, enables integrated decision-making

Source: elaborated by the student inspired by the the review

on the other hand ,and when talking about Cyber Risks in Geopolitical Contexts Figure 05 highlights the top cyber risks perceived by CEOs and CISOs in the context of escalating geopolitical tensions. Notably, *disruption of operations* (31% CEOs, 45% CISOs) and *cyber espionage* (33% CEOs, 27% CISOs) rank highest, indicating a shared concern for both immediate operational continuity and long-term strategic vulnerability. While CEOs appear more focused on strategic threats (espionage, cost), CISOs prioritize operational impact (disruption, reputation).

Figure 5 : The effects of geopolitical tensions on organizations' cybersecurity strategies



Source: (Canadian center for cybersecurity,2024, n.d.)

From a GRC perspective, this divergence emphasizes the need for integrated governance models that align board-level priorities with technical risk intelligence. Governance must elevate cyber risk to a strategic tier-one concern; risk management must address both systemic operational threats and silent, long-tail exposures like IP theft; compliance must evolve to account for geopolitical data flows, cross-border dependencies, and regulatory sovereignty. The following table maps each risk category to its GRC implications.

Table 12: GRC Analysis of Cyber Risks in Geopolitical Contexts

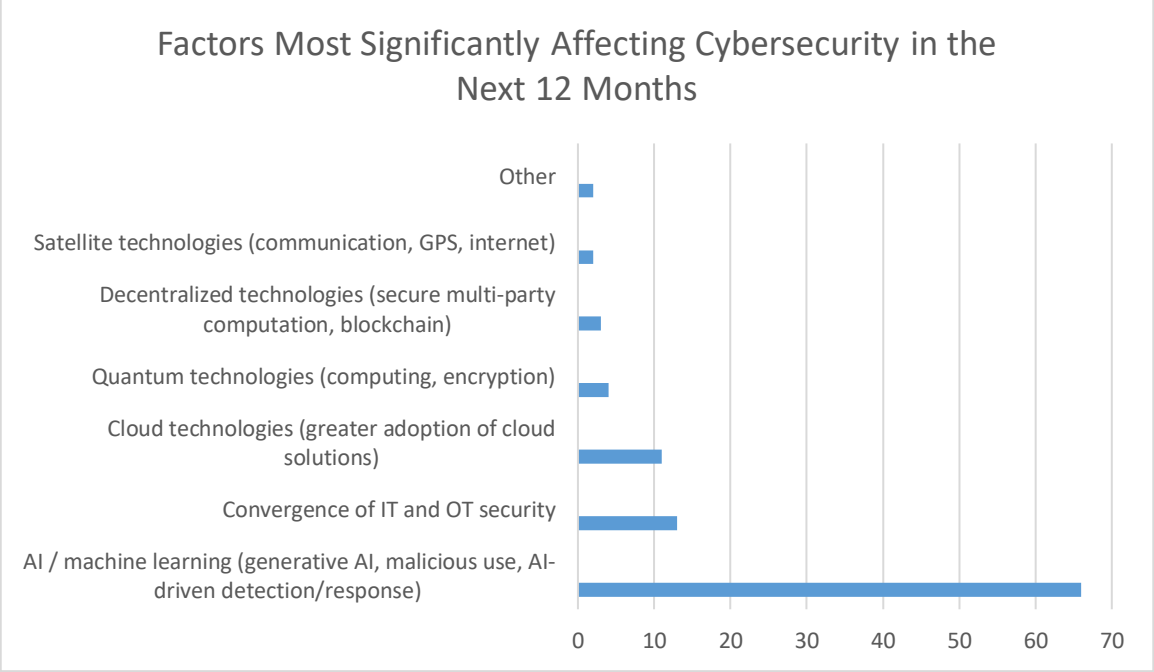
Cyber Risk	CEO Concern	CISO Concern	Governance	Risk Management	Compliance
Disruption of operations	31%	45%	Ensure continuity planning is board-level priority; define executive accountability	Conduct Business Impact Analysis (BIA); simulate disruptions; maintain backups	Require tested incident response and disaster recovery plans (ISO 22301, NIS2)
Cyber espionage / loss of sensitive info or IP	33%	27%	Protect strategic assets through clear data governance and IP ownership structures	Classify sensitive information; conduct insider threat and espionage risk assessment	Comply with IP law, export controls, and data localization regulations
Financial losses due to cyberattacks	11%	11%	Link cyber budgeting to strategic finance governance; involve CFO in security posture	Model financial exposure; integrate cyber insurance and loss forecasting	Meet financial reporting obligations post-breach (SOX, GDPR fines, etc.)
Damage to brand and loss of customer trust	7%	12%	Define external communication policies during incidents; involve PR and legal	Assess reputational risk; monitor sentiment and recovery timelines	Fulfill disclosure obligations to consumers and regulators (GDPR, PCI-DSS)

Cyber Risk	CEO Concern	CISO Concern	Governance	Risk Management	Compliance
Increased cybersecurity/incident response costs	8%	1%	Evaluate security investments at the board level; consider long-term efficiency	Prioritize resource allocation based on threat modeling	Maintain cost-effective security controls under compliance standards
Disinformation campaigns	5%	2%	Include media integrity and stakeholder manipulation in governance concerns	Monitor misinformation risk; assess social engineering vectors	Align with election law, platform policies, and content regulation frameworks
Not concerned	3%	2%	Indicates overconfidence or under-awareness in executive governance	Highlights need for cyber awareness training among top leadership	May imply non-compliance with mandatory risk assessment frameworks
Other	2%	1%	Governance must include emerging threat detection mechanisms	Risk teams should evaluate non-traditional threats continuously	Adjust compliance scope to include novel or emerging digital risks

Source: BY THE STUDENT INSPIRED FROM (Canadian center for cybersecurity,2024, n.d.)

The next figure(06) shifts the lens toward emerging vulnerabilities predicted to impact cybersecurity in the near future. A staggering 66% of professionals identify AI and machine learning technologies, both as security solutions and attack vectors, as the top risk area. Despite this, 63% of organizations still lack a formal AI security assessment process, exposing a critical governance and compliance gap.

Figure 6:Cybersecurity vulnerabilities in 2025 predicted by professionals



Source: BY THE STUDENT INSPIRED FROM (Canadian center for cybersecurity,2024, n.d.)

From a GRC standpoint, this illustrates a growing "AI-cyber paradox": organizations acknowledge AI-related threats but lag in establishing oversight mechanisms. Governance structures must integrate AI ethics, safety, and accountability at the board level. Risk management must incorporate generative AI into evolving threat models. Compliance needs to catch up, especially regarding AI explainability, bias mitigation, and audit trails. The convergence of IT and OT, cloud expansion, and quantum tech also reinforce the need for anticipatory GRC systems, proactive, adaptive, and embedded across digital infrastructures.

Table 13 :GRC Analysis of Emerging Cybersecurity Vulnerabilities in 2025

Predicted Vulnerability (2025)	**% of Professionals**	**Governance**	**Risk Management**	**Compliance**
AI / Machine Learning technologies	66%	Establish AI governance boards, define accountability for AI-related security	Integrate AI threats (e.g., deepfakes, AI-driven malware) into threat models	Ensure alignment with AI regulation, transparency, explainability, and auditability
Convergence of IT and OT security	13%	Extend security governance to physical	Identify vulnerabilities at IT-OT interfaces; implement cross-	Comply with sector-specific OT regulations (e.g.,

Predicted Vulnerability (2025)	% of Professionals	Governance	Risk Management	Compliance
		systems and OT environments	domain risk scenarios	NERC CIP, ISA/IEC 62443)
Cloud technologies	11%	Require strong governance of third-party and multi-cloud vendors	Assess data residency, availability, and platform misconfiguration risks	Apply cloud-specific standards (e.g., ISO/IEC 27017, CSA CCM, GDPR)
Quantum technologies (encryption, computing)	4%	Anticipate impact on cryptographic standards; fund quantum-readiness efforts	Monitor high-value assets vulnerable to quantum decryption	Ensure compliance with evolving encryption regulations and dual-use export laws
Decentralized technologies (blockchain, SMPC)	3%	Implement governance over distributed trust models and consensus mechanisms	Evaluate risks in smart contracts, key management, and interoperability	Address jurisdictional conflicts and smart contract legal enforceability
Satellite technologies (GPS, internet)	2%	Ensure governance includes space asset dependencies and positioning systems	Identify GPS spoofing, communication jamming, and data interception risks	Comply with national space/cyber defense policies and telecommunication laws
Other	2%	Encourage adaptive governance for unknown or hybrid threats	Include horizon scanning and early warning capabilities in risk processes	Remain flexible to integrate new standards and emerging regulatory frameworks

(Adedamola Oluokun, Adebimpe Bolatito Ige, et al., 2024)Source: BY THE STUDENT INSPIRED FROM (Canadian center for cybersecurity,2024,

n.d.)

Synthesis

This section demonstrates that GRC frameworks serve as both the architecture and the engine for cyber resilience in digital transformation. Across strategic integration, adaptive infrastructure, exposure management, and resilience-building, GRC unifies governance vision, risk intelligence, and compliance enforcement into a cohesive system. These frameworks allow organizations to not only withstand but adapt to the technical uncertainties of the digital age. By embedding GRC deeply across organizational layers—from boardrooms to backend systems—enterprises can operationalize security as a strategic function, ensuring agility, continuity, and trust. As the next section turns to broader discussions and reflections, this evidence affirms GRC's essential role in enabling secure and sustainable digital transformation.

Section 3: Review of Case Studies and Applied Contexts of GRC in Digital Transformation

The theoretical promise of Governance, Risk, and Compliance (GRC) frameworks in navigating digital transformation is undeniable. These frameworks are designed to align strategic objectives, manage risks, and ensure compliance in rapidly evolving digital environments. However, the implementation of GRC in practice often reveals gaps between theoretical expectations and real-world performance. This section explores empirical findings, real-life deployments, and illustrative case contexts to unpack the complexity and nuances of GRC in action.

A range of studies showcases GRC's implementation across diverse sectors and national settings. For instance, (Adedamola Oluokun, Adebimpe Bolatito Ige, et al., 2024)highlight how industry leaders such as PayPal and JPMorgan Chase utilize AI-enhanced cybersecurity strategies within a GRC framework to maintain operational integrity and regulatory compliance. (Deistler & Rentrop, 2022)) examine small and medium-sized enterprises (SMEs) in the EU and reveal that resource constraints often hinder holistic GRC adoption, resulting in fragmented governance and risk silos. Meanwhile, (Rebecca Pariela & Suparno, 2024) present a normative legal analysis of Indonesia's attempts to embed GRC into its legal and institutional frameworks, noting both progress and systemic inertia.

Further depth is added by (Nicolas Racz,*A Process Model for Integrated IT Governance, Risk, and Compliance Management*, n.d.), who propose an integrated IT GRC model but admit that their scenario remains largely hypothetical and untested in real conditions. The UN E-Government Survey (2024) (UNITED NATIONS 2024, 2024) provides macro-level perspectives with examples ranging from India's Aadhar system to broader evaluations of digital government readiness, revealing a spectrum of maturity in applying GRC at national levels. (Olorunyomi Stephen Joel et al., 2024) share insights from anonymized case studies, contrasting the successful digital transformation of a retail enterprise with the persistent struggles of a manufacturing firm grappling with outdated systems and workforce skill gaps. Complementing these examples(Vergara Cobos, 2024)presents a comprehensive analysis of cyber incidents and global attack patterns, including the Pemex ransomware case, reinforcing the critical need for proactive and dynamic GRC capabilities.

Several patterns recur across these studies. A primary challenge is the failure to fully integrate the three pillars of GRC, resulting in isolated efforts and lack of synergy. This fragmentation is often exacerbated by inconsistent reporting mechanisms, hidden implementation costs, organizational resistance to change, and poorly defined roles and responsibilities. The UN Survey (2024) underscores this by identifying persistent obstacles such as digital inequality, inadequate cybersecurity funding, and misalignment between policy design and execution.

Despite these shortcomings, successful implementations tend to share enabling conditions. These include engaged leadership, cross-functional communication, participatory stakeholder governance, and an organizational culture that values risk transparency and continuous learning. (Adebayo Adeyinka Victor et al., 2024; Adedamola Oluokun, Adebimpe Bolatito Ige, et al., 2024) emphasize that when GRC is championed from the top and woven into daily operations, it becomes a catalyst for resilience and innovation.

However, the disconnect between theory and practice remains stark. Scholars like (Karthick, 2023) call for more empirical studies to assess the effectiveness of GRC frameworks outside of theoretical modeling. Racz et al. (n.d.) acknowledge that real-world validation of their proposed models is still lacking. (Siahaan et al., 2023), focusing on anti-corruption frameworks, likewise point to the challenge of translating integrated GRC into measurable outcomes. Further complicating matters are issues of data scarcity in cybersecurity research (Vergara Cobos, 2024) and the rigidity of many frameworks that are ill-suited for highly dynamic or under-resourced environments.

(Kraus et al., 2021) add that socio-cultural variables, often underestimated in technical GRC models, play a major role in determining digital transformation outcomes. Costs, resistance to innovation, and institutional legacy systems are all factors that must be better integrated into GRC design.

Synthesis: What can we learn from past GRC applications, and where do they fall short in practice?

The accumulated evidence suggests that while GRC offers a robust conceptual structure for navigating digital transformation, its operational success hinges on strategic adaptation and contextual intelligence. Implementation failures often stem from a lack of integration across governance, risk, and compliance functions; underinvestment in cultural and human capital; and reliance on generic frameworks ill-suited to specific organizational or national realities.

Conversely, where GRC delivers value, it does so through strong leadership, tailored frameworks, transparent communication, and continuous monitoring. These factors help close the gap between intention and execution. The overarching insight is that GRC is not a static blueprint but a dynamic, context-sensitive capability. As such, future success in digital transformation will depend not just on adopting GRC frameworks but on embedding them meaningfully into the strategic DNA of organizations and institutions.

Conclusion

This literature review confirms that Governance, Risk, and Compliance (GRC) frameworks hold significant potential as strategic enablers that address the complex dual challenges organizations face during digital transformation: the human side—including resistance to change, technology acceptance, and organizational culture—and the technical side—namely cybersecurity risks and resilience.

While foundational GRC concepts (Adebayo Adeyinka Victor et al., 2024; Shahim et al., 2012) provide a basis, the literature reveals gaps in applying GRC holistically as a cultural and strategic driver rather than a mere compliance tool. GRC practices that promote transparency, ethical conduct, accountability, and effective communication have demonstrated promise in mitigating human resistance and fostering greater technology acceptance and agility (Doeze Jager et al., 2022; Magsamen-Conrad et al., 2022)). Simultaneously, established frameworks (ISO 27001, COBIT), increasingly enhanced by AI technologies (Benita Urhobo, 2024; McIntosh et al., 2023)), enable proactive management of cyber risks and the strengthening of cyber resilience.

However, the integration of AI into GRC introduces novel ethical, governance, and oversight challenges, emphasizing the need for responsible human moderation alongside automation. This emerging intersection highlights the evolving complexity of digital transformation governance.

Despite these insights, critical gaps remain, particularly a lack of rich, qualitative understanding of how organizations operationalize GRC to simultaneously navigate human and technical challenges, and how culturally informed, adaptable frameworks can be developed and sustained in diverse contexts.

Therefore, this study's inductive qualitative approach, employing expert interviews and case analyses, is well-positioned to fill these gaps. It aims to generate nuanced, actionable knowledge on GRC's strategic alignment with organizational culture and technology adoption, its role in managing AI integration ethically, and its practical impact on digital transformation success.

Chapter 02: Methodological Framework

This chapter presents the interpretivist, qualitative approach guiding our exploration of GRC in digital transformation. We employ two core methods: semi-structured expert interviews, including responses from both human and AI participants, and an embedded case study at the Algerian Ministry of Justice. Data collection in the case study involved participant observation, document analysis, and informal interviews. Analytical rigor is ensured through the use of Voyant Tools for text mining and the Gioia Methodology for inductive coding, enabling a rich, grounded understanding of both formal and informal GRC practices,as detailed below.

Section one: Philosophical and Methodological Foundations of the study

1. Epistemological and Methodological Paradigm

Our research is grounded in an **interpretivist epistemology**, which holds that knowledge of the social world is constructed through human interpretation, interaction, and shared meaning-making rather than discovered as objective fact (Crotty, 2020). This stance rejects positivist assumptions of fixed, measurable reality and instead recognizes reality as context-dependent, fluid, and shaped by lived experiences. Moreover, our literature review indicates that GRC is not "one-size-fits-all" but must be tailored to each organization's specific context and needs.

In studying the complex domain of governance, risk management, and digital transformation, it is critical to clarify three interrelated but distinct research components guiding our work:

- **Epistemology:** We adopt interpretivism, valuing subjective meanings and context-bound understanding—emphasizing how individuals and organizations construct knowledge through experience and social interactions ((Gioia et al., 2013).
- **Research Design:** We follow a qualitative, exploratory case study design, allowing flexible investigation of how GRC practices are enacted and adapted across different sectors and institutional settings (Yin, 2018).
- **Methodology/Methods:** Our study employs semi-structured interviews with experts, an embedded institutional case study at the Directorate of Modernization, Ministry of Justice, Algeria, and analysis via the Gioia Methodology to capture rich, grounded insights (Gioia et al., 2013)

This differentiation ensures conceptual clarity, aligning our epistemological stance with appropriate research design and methods to deeply understand GRC as a socio-technical phenomenon embedded in institutional cultures, professional norms, technological infrastructures, and power relations.

We focus on two interrelated dimensions of GRC as enablers of digital transformation:

- **Technical dimension:** cybersecurity strategies, digital infrastructure, regulatory controls.
- **Human dimension:** change management, employee engagement, technology adoption, resistance.

These dimensions cannot be fully captured through quantitative metrics or general models. Instead, they require a qualitative, context-sensitive approach that uncovers how professionals and institutions perceive, experience, and make sense of GRC's role.

Accordingly, we adopt a constructivist–interpretivist framework, privileging practice-based understanding over prediction (Denzin & Lincoln, 2018) and using inductive reasoning to allow new conceptual insights to emerge directly from the data.

To ensure analytical rigor, we apply the Gioia Methodology (Gioia et al., 2013), a structured inductive process that supports:

- Capturing participant meaning through first-order concepts;
- Interpreting patterns via second-order themes;
- Synthesizing aggregate dimensions that contribute to novel theoretical framing.

This approach aligns seamlessly with our epistemological, methodological, and exploratory objectives, enabling rich contextual analysis and the emergence of new conceptual insights relevant to digital governance, risk, and compliance

2. Research Design

This study employs a qualitative, exploratory research design grounded in (Yin, 2018)case study framework, which is well-suited to answering "how" and "why" questions in real-world organizational contexts. By combining semi-structured expert interviews and an embedded case study, we achieve both breadth and depth:

2.1 Semi-Structured Expert Interviews

- **Purpose:** To explore cross-sectoral perspectives on GRC adoption, its perceived usefulness, and its role in addressing digital transformation challenges.
- **Scope:** Seven experts from diverse sectors (public, private, NGOs, academia) occupying strategic, advisory, or managerial roles in digital transformation, cybersecurity, governance, risk management, or compliance.
- **Rationale:** Provides horizontal thematic exploration, capturing varied experiences and industry best practices.

2.2 Embedded Case Study at the Directorate of Modernization, Ministry of Justice, Algeria

- **Purpose:** To investigate in depth how a key regulatory institution operationalizes GRC practices, both formal and informal, within its unique institutional environment.
- **Scope:** Multiple sub-units, including IT & Cybersecurity, Compliance & Legal Affairs, and E-Justice Platforms.
- **Rationale:** Offers vertical, contextualized understanding of GRC enactment under stringent regulatory and security demands.

This mixed-methods approach enables methodological triangulation, enhancing the credibility and validity of our findings. It supports iterative refinement of a two-path conceptual framework that links the technical dimension (cybersecurity, infrastructure, controls) with the human dimension (change management, engagement, adoption, resistance) of GRC in digital transformation

Section Two: Data Collection Methods

We employ a dual-method qualitative data collection strategy**,** semi-structured expert interviews and an embedded case study, to capture both broad, cross-sector insights and in-depth, context-specific understanding of GRC practices. By integrating these two methods, we ensure thematic breadth (experts' perspectives across industries) and contextual depth (detailed examination within a single institution). This combination strengthens triangulation, enriches our analysis, and supports the development of robust, grounded theory.

1. Semi-Structured Expert Interviews

1.1 Human Experts

- **Participants:** Seven subject-matter experts with strategic, advisory, or managerial roles in digital transformation, cybersecurity, governance, risk management, or compliance.

We used purposive, criterion-based sampling to select information-rich experts and ensure diversity of experience and perspective:

- **Inclusion Criteria:**
    - Minimum five years' experience in digital transformation, cybersecurity, governance, risk management, or compliance.
    - Strategic, advisory, or managerial roles with direct involvement in GRC decision-making.
    - Representation across sectors: public administration, private enterprise, NGOs, and academia.
- **Sample Size:** Seven experts, thematic saturation was achieved by interview five, with subsequent interviews yielding no new substantive insights. This early saturation is supported by the homogeneity of expertise and the depth of discussion (Guest et al., 2020);(Marshall et al., 2013).

Table 14 : Participant Profiles

ID	Role	Sector	Experience (yrs)	Expertise
E1	Chief Information Security Officer	Financial Services	12	Cybersecurity
E2	Director of Digital Transformation	Manufacturing	10	Change Management
E3	Compliance Manager	Healthcare	20	Regulatory Compliance
E4	IT Governance Lead	Energy	16	IT Governance
E5	Risk Management Consultant	Consulting	11	Risk Assessment
E6	Academic Researcher	University	19	Organizational Learning
E7	Cybersecurity company'sCEO	Cybersecurity	10	Digital Strategy

Source: elaborated by the student

1.2 AI Models

1.2.1 AI Expert Selection and Consistency Control

The selection of AI models for expert interviews was guided by the following criteria:

- Diversity of Capabilities and Design Philosophy: We selected four AI models (ChatGPT, DeepSeek, Studio AI, and Copilot) that represent different approaches to large language model development and deployment. This diversity ensured a range of perspectives rather than relying on a single AI architecture or training methodology.
- Complementary Specializations: Each selected AI model offers distinct strengths relevant to our research domain:
    - ChatGPT: Broad knowledge base and conversational capabilities.
    - DeepSeek: Enhanced reasoning and academic/research orientation.
    - Studio AI: Creative problem-solving and platform-agnostic solutions.
    - Copilot: Enterprise integration and practical implementation focus.

- Accessibility and Reproducibility: All selected models are publicly available, allowing for verification and reproduction of our methodology by other researchers.
- Technical Maturity: Each model had demonstrated capabilities in complex reasoning and domain-specific knowledge generation, as evidenced by published benchmarks and peer-reviewed evaluations.
- Recency of Training Data: Models with more recent training data were prioritized to ensure familiarity with current GRC frameworks, cybersecurity threats, and digital transformation challenges.

1.2.2. Consistency Control Measures

To ensure consistency in the AI-generated responses and facilitate meaningful comparison with human experts, we implemented the following controls:

- Standardized Prompting Protocol: All AI models received identical interview questions using the same expert interview guide applied to human participants. Each prompt was prefaced with the same role instruction:
  - "Act as a digital transformation expert with over 15 years of domain experience, having guided diverse sectors in IT implementation with a background in GRC."
- Controlled Context Window: We maintained consistent context windows across all AI interactions, ensuring that each model had access to the same background information and previous question-answer pairs.
- Blind Evaluation: During the initial analysis phase, we coded and analyzed AI-generated responses without knowledge of which model produced them, reducing potential bias in interpretation.

These methodological controls ensured that variations in AI responses reflected genuine differences in model capabilities and approaches rather than inconsistencies in how the models were prompted or deployed.

1.3. Interview Guide Structure

Our interview guide followed this structure:

- **Section A: Organizational Practices & Technology Acceptance:** Questions on factors influencing technology adoption, leadership support, and communication strategies.

- **Section B : Risk Thinking & Cyber Resilience:** Questions on technical, human, and procedural risks; organizational preparedness; and resilience practices.
- **Section C: Strategy, Structure & Institutional Learning:** Exploration of organizational features that support or hinder transformation, proactive risk mindsets, and core governance elements.
- **Optional Reflection:** A framing question on whether GRC pillars resonate in practice under different terms or forms.

Source & Inspiration: The guide was adapted from the UTAUT model (Venkatesh et al., 2003) and Kotter's 8-Step Change Model (Kotter, 1996) to ensure validity in technology acceptance and change management queries. Technical-risk questions draw on the NIST Cybersecurity Framework and ISO/IEC 27001 control objectives (National Institute of Standards and Technology, 2018).

Differentiation: This expert guide focuses on sector-agnostic themes, whereas the case study protocol is tailored to institutional processes and uses conversational interviews to capture informal practices.

2. Embedded Case Study

2.1. Why the Directorate of Modernization, Ministry of Justice, Algeria?

- **Compliance Expertise:** As architects of legal and regulatory frameworks, the Directorate possesses unparalleled insight into designing, enforcing, and interpreting IT related policies.
- **Sensitive Data Management:** It oversees highly confidential justice-sector data, requiring stringent cybersecurity and compliance measures.
- **Institutional Complexity:** Its multifaceted organizational structure and public accountability create a rich environment for studying the interaction of formal and informal GRC practices.

2.2. Methods of Collecting Case Study Data

- **Participant Observation:** Conducted during a three-month internship, we observed leadership meetings, risk-assessment workshops, and compliance audits, capturing both formal procedures and informal routines in real time.

- **Document Analysis:** Reviewed internal strategy reports, compliance protocols, security audit findings, and policy manuals to map the Directorate's formal GRC framework.
- **Conversational Interviews:** Held unstructured, informal interviews with key personnel (managers, technical staff, legal advisors) to surface tacit knowledge and informal GRC practices not codified in documents.

This triangulated data collection approach ensures a comprehensive view of how GRC is practiced, both formally and informally, within the Directorate of Modernization.

Section three: Data Analysis Approach

Our analysis employs two parallel strands—one for the semi-structured expert interviews and one for the embedded case study—before integrating findings into a cohesive framework.

1. **Semi-structured Expert Interviews**

1.1.Text Analysis

- **Word Cloud Generation:** We created word clouds from interview transcripts to visualize the most frequently used terms, highlighting core concepts such as "risk," "governance," "adoption," and "resilience."
- **Line Graphs of Theme Saturation:** We plotted the emergence of key themes across interviews to confirm that by the fifth interview, no new major themes surfaced, validating thematic saturation**.**

Use of Voyant Tools for Text Analysis

In this study, Voyant Tools was employed for text analysis to efficiently explore and extract insights from the data. Voyant is a web-based application that allows for the analysis of large volumes of text, providing visualizations like word clouds and frequency graphs to identify key patterns and trends.

Justification for the Use of Voyant Tools

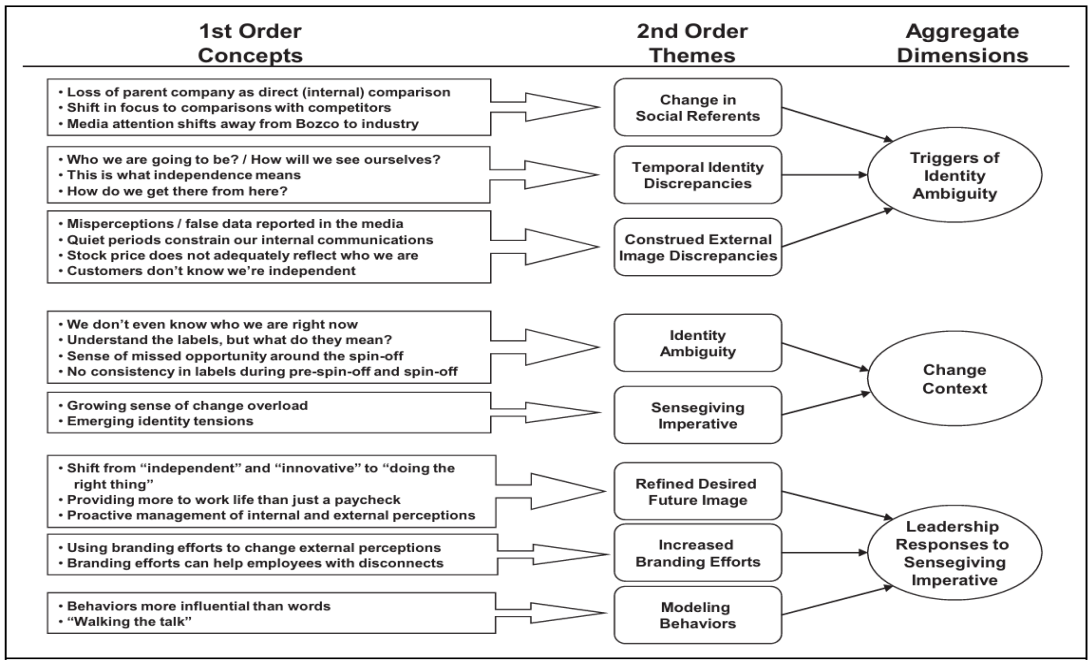
- **Efficiency**: Voyant Tools allows for quick analysis of large datasets, making it ideal for handling extensive textual data.
- **Visualization**: Its ability to generate interactive visualizations aids in the identification of significant terms and themes, enhancing data interpretation.
- **Contextual and Frequency Analysis**: The tool supports both word frequency analysis and contextual exploration, allowing for deeper insights into term relationships and patterns.
- **Support for Inductive Research**: Voyant Tools' flexibility aligns with the inductive nature of the study, enabling exploratory analysis without predefined categories.
- **Reproducibility**: The tool's transparent outputs ensure that the analysis process is clear and replicable by other researchers.

1.2. Gioia Methodology

We then applied the Gioia Methodology in three stages:

- **First-Order Concepts:** Extracted informant-centric codes directly from transcripts (for example: “leadership buy-in,” “compliance anxiety,” “digital resistance”).
- **Second-Order Themes:** Organized these codes into researcher-centric themes (for example: “organizational trust,” “regulatory burden,” “change agency”).
- **Aggregate Dimensions:** Synthesized themes into high-level dimensions underpinning our conceptual framework (for example: “Adaptive Governance,” “Resilience Engineering,” “Change Enablement”**).**

figure 7: data structure



Source : (Gioia et al., 2013)

2. Embedded Case Study

2.1.Diagnosing Using the ACADYC Method

We utilized the **ACADYC framework** (a diagnostic tool for Assessing CApability, DYnamics, and Change) to evaluate the Directorate’s institutional maturity, identifying strengths, gaps, and development areas across governance, risk, and compliance functions.

*2.2.*Formal vs. Informal GRC Practices Lens

- **Formal Practices:** Coded and analyzed documented policies, protocols, and audit procedures to map official GRC architecture.
- **Informal Practices:** Identified through observation notes and conversational interviews, tacit routines such as peer-to-peer risk escalation, ad-hoc compliance checks, and informal decision forums.

By contrasting these two lenses, we diagnosed how informal behaviours either supported or subverted the formal GRC framework, revealing opportunities for integration and improvement.

This dual analysis approach ensures both depth (case study diagnostics) and breadth (cross-sector interviews), culminating in a robust, grounded understanding of GRC in digital transformation contexts.

Chapter 03: Presentation and Analysis of Results

This chapter presents the results of the study based on the data collected through expert interviews and the embedded case study. The findings are structured to reflect the core themes that emerged from both sources, offering a clear view of how GRC is perceived and practiced in the context of digital transformation.

Section One: Semi-Structured Expert Interviews

This section presents a comprehensive analysis of expert insights derived from two distinct sources: human expert interviews and AI-simulated expert interviews. The objective is to explore how Governance, Risk, and Compliance (GRC) frameworks enable digital transformation, foster technology acceptance, and enhance cyber resilience.

Both data sources underwent rigorous textual and thematic analyses to extract converging and diverging themes. The inclusion of AI-generated perspectives is both methodologically and contextually justified. Notably, the literature emphasizes the emerging role of AI in shaping and implementing GRC policies. As AI tools become increasingly integrated into strategic decision-making, simulating expert responses through AI offers a forward-looking dimension, highlighting not only current practices but also evolving possibilities.

1. Text Analysis

1.1. Word Cloud Visualization

1.1.1. Human-Based Interviews

Figure 8: The word cloud derived from human expert transcripts

Source: elaborated by the students using voyant tools

The word cloud derived from human expert transcripts prominently features terms such as digital, leadership, transformation, risk, security, support, accountability, culture,

communication**,** and adoption**.** This lexical distribution reflects the experts' strong emphasis on leadership visibility, risk management, organizational culture, and the critical role of communication in change processes**.**

1.1.2. AI-Stimulated Interviews

Figure 9: The word cloud derived from AI-generated ranscripts

Source: elaborated by the students using voyant tools

The AI-generated word cloud shows overlapping but nuanced emphasis on leadership, digital, communication, resistance, adoption, governance, change, and training**.** Notably, resistance and adoption are visually more prominent than in the human cloud, indicating AI's heightened attention to behavioral change and adoption dynamics**.** This may derive from AI's exposure to broader change management literature. The AI also explicitly includes governance and organizations**,** emphasizing formal structural aspects of GRC alongside cultural themes.

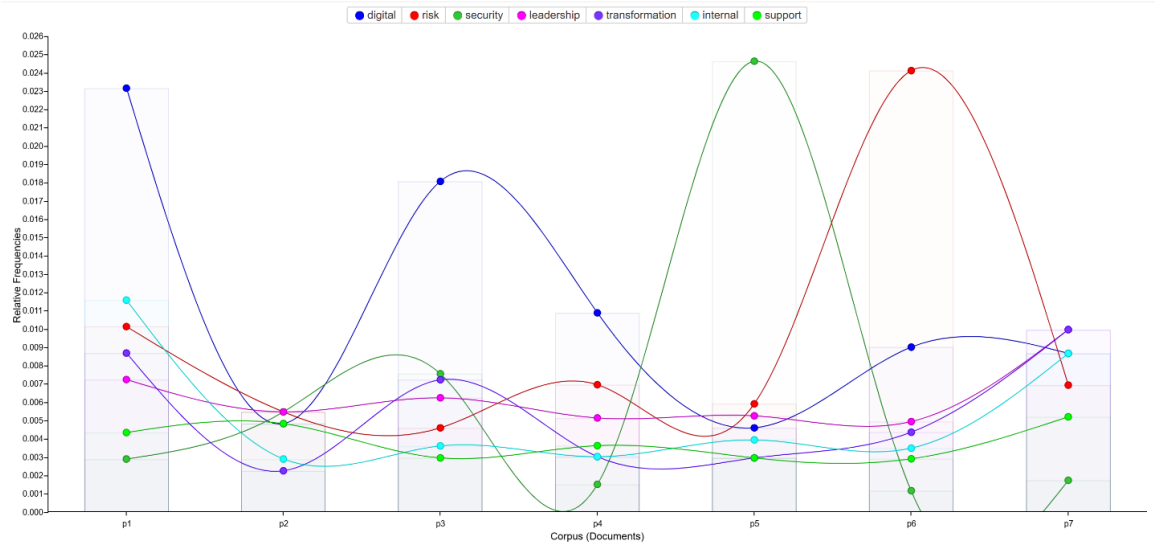
1.1.3. Interpretation of Word Clouds

Both human and AI word clouds highlight core themes of leadership and digital transformation, with risk and security as foundational concerns. The AI's additional focus on resistance and communication suggests its training on broader change management literature, complementing expert lived experience by emphasizing stakeholder engagement and behavioral dynamics.

1.2. Frequency of Key Concepts Across Experts and AI Models

1.2.1. Human-Based Interviews

Figure 10: Frequency of Key Concepts Across experts



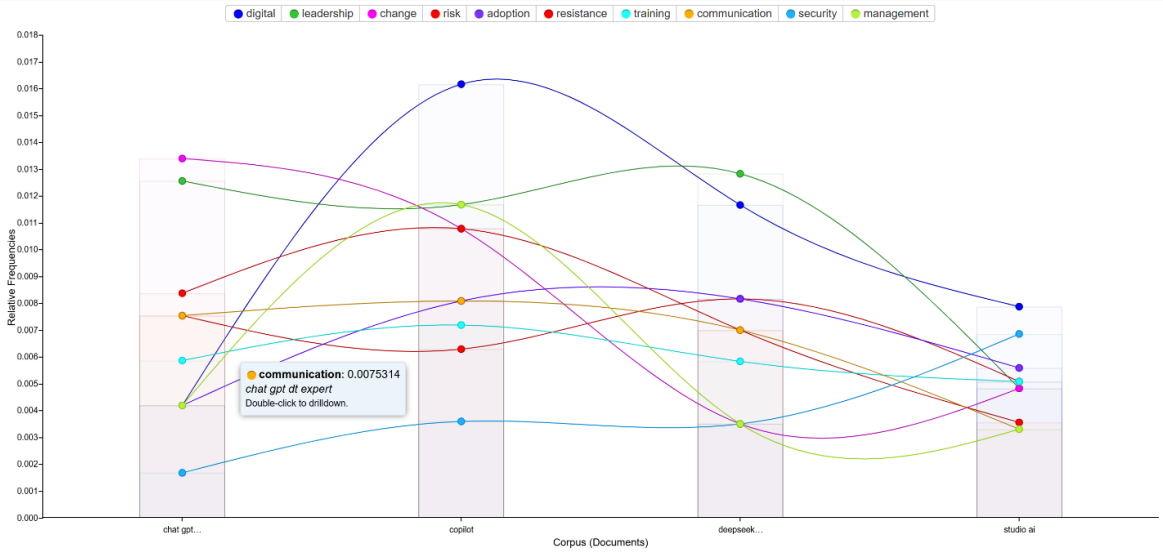
Source: elaborated by the students using voyant tools

The frequency line graph illustrates keyword usage across seven distinct human experts (P1 through P7), each with unique expertise and focus areas. Terms like "digital" and "transformation" are most prominent in experts P1 and P3, indicating their strong engagement with overarching digital change narratives. Expert P6 shows a peak in "risk", reflecting specialization in security and risk management, while P5 emphasizes "support", pointing to organizational enablement or technical assistance. Variations in terms such as "leadership" and "security" reveal diverse professional roles and viewpoints within the broader GRC and digital transformation ecosystem.

This distribution demonstrates how thematic emphases differ according to the experts' backgrounds, illustrating the multifaceted nature of governance and digital transformation challenges.

1.2.2. AI-Stimulated Interviews

Figure11: Frequency of Key Concepts Across AI simulated interviews



Source: elaborated by the student using voyant tools

The AI-generated frequency graphs reveal distinctive thematic focuses across models. For example, Copilot strongly emphasizes digital themes, while DeepSeek accentuates leadership. ChatGPT highlights resistance and communication, showcasing interpretative nuances. These distinctions show that AI models, while aligned with human themes, offer complementary perspectives emphasizing different aspects of digital transformation.

1.2.3. Interpretation

The varied frequencies across experts and AI models indicate that while core themes like digital transformation and risk management are shared, AI models expand focus towards behavioral and cultural elements. This enriches understanding by layering human expertise with AI-generated insights.

1.3. Comparative Analysis of Human vs AI Textual Outputs

The textual analyses collectively reveal strong thematic alignment on leadership, risk, culture, and governance, validating the domain's core priorities. Differences lie in the AI's stronger articulation of communication, resistance management, and formal governance frameworks, offering complementary insights that extend human expert findings. This triangulation enhances analytical robustness

2. GIOIA-Based Data Analysis

2.1. Human and AI-Stimulated Coding and Presentation

2.1.1. Human Interview Coding and Presentation

Table 15:Human Interview data structure

Aggregate Dimension	Second-Order Theme	Selected Quotations
Strategic & Agile Governance	Sustained & Visible Leadership	"Top leadership support, visibility, strategic clarity." (Expert 3)
	Structured Rollouts & Governance	"Structured roadmap, phased rollouts, team involvement." (Expert 2)
	Informal Security Culture	"Security champions, open reporting." (Expert 5)
	Safe Reporting & Culture	"Punishing reports stops reporting." (Expert 4)
	Iteration & Learning by Doing	"Post-mortems, reflection." (Expert 6)
	Cyber Preparedness & Practice	"Incident response plans, simulations." (Expert 2)
Proactive & Holistic Risk Mgmt	Human-Centered Risk Awareness	"Human error, social engineering, insider threats." (Expert 4)
	Alignment with Values	"GRC aligns with organizational values." (Expert 2)
GRC as Strategic Enabler	From Policy to Practice	"Governance as active decision-making." (Expert 3)
	Clarity & Internal Communication	"Clear vision reduces resistance." (Expert 6)
Empowered, Learning, Security Culture	Empowerment & Role Clarity	"Agile teams, ownership at front lines." (Expert 1)

Source: elaborated by the student

This table summarizes the key themes and dimensions derived from the human expert interviews.

- Aggregate Dimension: Strategic & Agile Governance

  The experts emphasize sustained and visible leadership as crucial to driving transformation, highlighting the importance of ongoing executive commitment and strategic clarity. The theme of structured rollouts and governance reflects a methodical approach to transformation implementation, with clear roles and phased execution. Internal communication is also recognized as essential to minimize resistance and build understanding. Illustrative quotes such as "Top leadership support, visibility, strategic clarity" (Expert 3) and "Clear vision reduces resistance" (Expert 6) encapsulate these points.

- Aggregate Dimension: Proactive & Holistic Risk Management

  Human experts acknowledge the significance of human-centered risks, including social engineering and insider threats, balanced with technical preparedness measures such as incident response planning and simulations. The inclusion of informal security culture themes reveals the role of grassroots security champions and open reporting practices in cultivating resilience. Exemplary quotes include "Human error, social engineering, insider threats" (Expert 4) and "Security champions, open reporting" (Expert 5).

- Aggregate Dimension: Empowered, Learning, and Security-Conscious Culture

  This dimension illustrates a culture characterized by empowerment and role clarity, where agile teams assume ownership. The process of iteration and learning through reflection and post-mortems fosters continuous improvement. The theme of safe reporting underscores the need for a psychologically secure environment to encourage transparency, as shown by quotes like "Agile teams, ownership at front lines" (Expert 1) and "Punishing reports stops reporting" (Expert 4).

- Aggregate Dimension: GRC as Strategic Enabler

  Experts view GRC not merely as compliance but as a strategic, embedded governance mechanism. Themes such as from policy to practice and alignment with organizational values suggest that effective governance integrates into organizational

culture and decision-making processes. The quote "Governance as active decision-making" (Expert 3) reflects this dynamic understanding.

2.1.2. AI-Stimulated Interview Coding and Presentation

Table 16:AI-Stimulated Interview data structure

Aggregate Dimension	Second-Order Theme	Selected Quotations
Leadership as Change Catalyst	Executive Sponsorship & Championing	"Executives must champion the initiative." (Copilot)
	Transparent Multi-Channel Communication	"Explain the 'why' and 'how'—WIIFM." (ChatGPT DT Expert)
	Empowering Change Agents & Super-Users	"Super users as first-line support." (Studio AI)
Risk Intelligence & Resilience	Proactive Technical Controls	"Penetration testing, zero-trust architecture." (DeepSeek)
	Human Behavior & Awareness Bridging	"Phishing simulations and workshops." (DeepSeek)
	Informal Adaptive Defense Mechanisms	"Peer-led red teams." (ChatGPT DT Expert)
Continuous Learning & Adaptive Culture	Role-Specific Training & Support	"Ongoing accessible training." (Studio AI)
	Psychological Safety & Non-Punitive Reporting	"Culture encourages vigilance." (Copilot)
	User-Centric Involvement & Feedback Loops	"Users involved reduce resistance." (Studio AI)
Agile GRC Integration & Dynamic Compliance	Embedded Operational Practice	"GRC embedded, not checklist." (DeepSeek)
	Balancing Regulation with Innovation	"Compliance balanced with innovation speed." (DeepSeek)

	Culture-Driven Accountability & Ownership	“Informal GRC more effective.” (DeepSeek)

Source: elaborated by the student

This table reflects thematic dimensions derived from AI-simulated expert inputs.

Aggregate Dimension: Leadership as Change Catalyst. AI responses emphasize executive sponsorship and active leadership that champions change initiatives. They highlight the necessity of transparent multi-channel communication to convey the rationale behind transformations and the value to individuals. Empowering change agents and super-users is also a recurrent theme, facilitating adoption. For instance, "Executives must champion the initiative" (Copilot) and "Explain the ‘why’ and ‘how’,WIIFM" (ChatGPT DT Expert) exemplify this focus.

Aggregate Dimension: Risk Intelligence & Resilience. The AI coding reveals a nuanced blend of proactive technical controls such as penetration testing and zero-trust architectures, combined with human behavior and awareness efforts like phishing simulations. AI also identifies informal adaptive defense mechanisms, including peer-led red teams, indicating an understanding of evolving security cultures. Supporting quotes include "Penetration testing, zero-trust architecture" (DeepSeek) and "Phishing simulations and workshops" (DeepSeek).

Aggregate Dimension: Continuous Learning & Adaptive Culture. AI models consistently underscore role-specific training and support, along with fostering psychological safety and non-punitive reporting. The importance of user-centric involvement and feedback loops highlights an adaptive organizational culture focused on continuous improvement. Examples are "Ongoing accessible training" (Studio AI) and "Users involved reduce resistance" (Studio AI).

Aggregate Dimension: Agile GRC Integration & Dynamic Compliance. AI perspectives frame GRC as an embedded operational practice that balances regulatory compliance with the need for innovation agility. Themes of culture-driven accountability and ownership emphasize the importance of governance rooted in organizational culture rather than bureaucracy. Quotes such as "GRC embedded, not checklist" (DeepSeek) and "Compliance balanced with innovation speed" (DeepSeek) illustrate this approach.

2.1.3. Comparative Insights

Table 17 :comparative insights between human and AI simulated interviews

Aspect	Human Experts	AI-Simulated Experts	Commentary
Leadership Focus	Leadership as visible sponsor and culture builder	Leadership as multi-layered communication & empowerment	Human experts emphasize leadership's role as a visible, trusted sponsor shaping culture and strategic direction. AI elaborates with detailed communication tactics and empowerment at multiple organizational levels.
Governance	Agile, adaptive governance boards & roles	Formalized, operational governance frameworks	Humans highlight flexible, context-sensitive governance structures that evolve with transformation needs. AI complements this with detailed, formal frameworks that support operational decision-making.
Risk Management	Holistic sociotechnical risk culture	Integrated technical controls and adaptive culture	Human insights focus on the interplay between human behavior and security culture, valuing informal mechanisms. AI provides more explicit attention to technical controls while recognizing cultural adaptation.
Culture & Learning	Psychological safety, empowerment, reflection	Role-tailored training, psychological safety, feedback loops	Human experts stress lived experience of empowerment and safe environments for learning. AI supplements with structured training programs and systematic feedback to support adaptation.
GRC Role	Embedded, strategic, value-aligned	Operational, dynamic, innovation-balanced	Humans perceive GRC as embedded in values and organizational identity, enabling strategic alignment. AI frames GRC as a dynamic, agile practice balancing compliance with innovation demands.

Source: elaborated by the student

There is a strong overlap in core themes across human and AI-derived tables, notably leadership, risk management, culture, and GRC's role. However, nuances exist:

- Leadership Focus: Human experts emphasize leadership as a visible, trusted sponsor who not only provides strategic direction but actively shapes organizational culture. Their accounts focus on the criticality of leadership presence to build trust and guide transformation efforts. AI outputs complement this by elaborating on leadership's communication at multiple organizational levels and empowerment of change agents, offering a more granular and tactical perspective.

- Governance: The human expert narratives center on agile and adaptive governance structures, such as governance boards and clearly defined roles that evolve with the transformation process. This highlights their appreciation for flexibility and responsiveness in governance to meet changing organizational needs. AI-generated themes, meanwhile, detail more formalized and operational governance frameworks, underscoring structures that enable effective decision-making and control.
- Risk Management: Human experts present risk management as a holistic sociotechnical phenomenon, emphasizing the role of human behavior, culture, and informal security champions alongside technical measures. This suggests a deep appreciation of the interplay between people and technology in managing risk. The AI responses reinforce this but add explicit focus on technical controls such as penetration testing and zero-trust architectures, reflecting its grounding in technical literature.
- Culture & Learning: Human interviewees highlight the importance of psychological safety, empowerment, and reflective learning practices drawn from their real-world experiences. They emphasize creating environments where employees feel safe to report issues and continuously improve. AI simulations add value by specifying role-tailored training programs and systematic feedback loops, offering a structured view of how learning and culture can be operationalized.
- GRC Role: For human experts, GRC is deeply embedded in organizational values and strategy, acting as a strategic enabler rather than a mere compliance function. They see it as integral to organizational identity and decision-making. AI responses describe GRC as operational and dynamic, balancing regulatory requirements with innovation pressures, framing it as an agile practice embedded in daily operations.

3. Critical Reflection: AI vs. Human Expert Contributions

3.1. Convergent Themes Across AI and Human Experts

Despite their differing origins, both AI-generated insights and human expert interviews revealed key areas of convergence. These common themes highlight shared understandings regarding the role of GRC in digital transformation:

- Strategic Alignment as a Success Factor: Both sets of experts emphasized that GRC frameworks must be strategically aligned with organizational goals to effectively support transformation, rather than hinder it.
- Importance of Organizational Culture: A "risk-aware" culture was consistently identified as a prerequisite for effective GRC implementation, in contrast to a rigid, compliance-driven mindset.
- Integration of Formal and Informal Practices: Both groups acknowledged that formal structures alone are insufficient; informal, unwritten practices play a crucial role in how GRC actually functions.
- Balance Between Security and Usability: There was strong consensus that excessive security measures can backfire by undermining user experience and slowing adoption.

3.2. Divergent Perspectives Between AI and Human Experts

However, several critical distinctions emerged between AI-generated outputs and human interviews, revealing complementary but different lenses:

- Contextual Nuance: Human experts offered rich, real-world scenarios, while AI models presented idealized, generalized cases with less contextual depth.
- Emotional and Political Awareness: Human insights were often emotionally grounded, referencing power struggles, interpersonal dynamics, and resistance to change, elements that AI discussed only abstractly.
- Practical Adaptations: Workarounds, compromises, and informal adaptations were common in human narratives, while AI maintained adherence to formal models and frameworks.
- Regional and Cultural Specificity: Human experts, particularly those with Algerian experience, highlighted local realities and cultural constraints not captured in the more universalized AI narratives.
- Emerging and Experimental Practices: Humans were more likely to cite cutting-edge or undocumented practices, whereas AI reflected only what was available in existing literature and training data.

3.3. Comparative Strengths of AI Expert Contributions

AI-generated insights brought several analytical strengths that enhanced the research process:

- Breadth and Coverage: AI provided exhaustive references to frameworks, standards, and methodologies, often broader than what individual human experts could offer.
- Consistency in Theoretical Orientation: AI responses remained theoretically grounded throughout, whereas humans occasionally diverged into practical anecdotes that lacked academic anchoring.
- Synthesis of Diverse Sources: AI integrated perspectives across disciplines and frameworks, offering a panoramic view of the GRC landscape.
- Freedom from Stakeholder Bias: Unlike human experts, AI displayed no institutional or personal bias, providing neutral assessments without self-interest.
- Structured and Codable Responses: AI responses followed a clear and systematic logic, facilitating cleaner coding and cross-case comparison.

3.4. Comparative Strengths of Human Expert Contributions

Conversely, human experts offered irreplaceable value in specific domains:

- Contextual Intelligence: Human reflections were deeply embedded in organizational realities, revealing how GRC plays out amid socio-political dynamics.
- Tacit Knowledge: Practical wisdom, informal rules, and lived experience, often absent in formal literature, were central to human contributions.
- Creative and Adaptive Thinking: Humans navigated uncertainty and ambiguity with flexibility, offering novel solutions to unprecedented problems.
- Ethical and Political Sensitivity: Human experts were better equipped to assess ethical dilemmas and navigate power asymmetries within organizations.
- Critical Evaluation of Established Norms: Unlike AI, human experts were more willing to critique and adapt frameworks, suggesting modifications based on experience rather than theory alone.

3.5. Risks of Over-Reliance on AI in Future GRC Frameworks

While AI contributions are valuable, an overemphasis may introduce significant risks to GRC development:

- Loss of Tacit and Lived Knowledge: AI depends on documented input and may overlook crucial experiential insights that determine real-world success.
- Homogenization of Practices: Uniform AI-driven models may ignore cultural or organizational uniqueness, resulting in one-size-fits-all solutions.
- Innovation Stagnation: AI is excellent at synthesizing what is known but struggles to generate genuinely novel approaches or anticipate emerging trends.
- Ethical Oversimplification: Nuanced ethical dilemmas often require emotional and political judgment, which AI cannot replicate reliably.
- Abstraction from Reality: Idealized AI frameworks may ignore the implementation complexities and trade-offs highlighted by human experts.
- Reinforcement of Existing Biases: AI trained on Western-centric literature may inadvertently propagate systemic biases and marginalize non-Western or SME-specific concerns.
- Reduced Stakeholder Engagement: Bypassing human consultation for AI analysis risks alienating stakeholders, weakening commitment to GRC implementation.

Section Two: Case Study – Directorate of Modernization, Ministry of Justice, Algeria

This section presents an embedded case study centered on the General Directorate for the Modernisation of Justice within the Algerian Ministry of Justice. As the institutional nucleus for digital transformation initiatives in the justice sector, the Directorate provides a relevant and strategic context for examining Governance, Risk, and Compliance (GRC) practices in action. The objective is twofold: (1) to explore how formal and informal GRC mechanisms are embedded within its structures, and (2) to assess their impact on technology acceptance, cyber resilience, and adaptive change management.

The case study operationalizes the theoretical constructs of GRC by applying the first phase of the ACADYC methodology—diagnosing the current landscape of governance and control. Drawing from document analysis, interviews, and participant observations, this diagnosis surfaces the practical challenges and opportunities the Directorate faces in aligning its digital ambitions with secure, compliant, and accountable governance structures.

1. Presentation of the Directorate of Modernization -Ministry of Justice

This subsection provides an overview of the organizational context for the case study: the Directorate of Modernization within the Algerian Ministry of Justice. Understanding its formal structure and mandate is essential before diagnosing its governance, risk management, and compliance practices.

1.1 Institutional Context and Strategic Importance

Established by Executive Decree No. 02-410 and later restructured by Executive Decree No. 04-333, the General Directorate for the Modernisation of Justice was mandated to modernize the judicial system in terms of internal functioning, organizational efficiency, and integration with both national and international environments. This institutional effort was catalyzed in October 1999 by the creation of the National Commission for Justice Reform**,** whose extensive diagnostic work laid the foundation for Algeria's justice sector modernization strategy.

The Directorate operates under the direct supervision of the Minister of Justice, reflecting its high-level strategic role. Its responsibilities include:

- Proposing actions and mobilizing resources for modernization.
- Standardizing administrative and judicial procedures.
- Promoting digital tools and communication systems.
- Ensuring information security and cyber resilience.

The Directorate's work contributes directly to a broader national goal: the establishment of a justice system that is modern, accessible, efficient, and aligned with international best practices.

1.2 Organizational Structure and Key Departments

The General Directorate is composed of two principal departments, each housing multiple sub-directorates that address both technical and organizational dimensions of justice modernization.

A. Directorate of Information Technology and Communication (ITC)

This department spearheads the technological transformation of the justice system. It introduces digital tools, manages ICT infrastructure, and ensures cybersecurity across judicial entities.

Key responsibilities include:

- Overseeing the deployment and maintenance of justice IT networks.
- Automating administrative and judicial procedures.
- Managing software solutions and IT systems.
- Ensuring the cybersecurity of critical systems.
- Promoting internal and external digital communications.

Sub-directorates:

- **IT Systems:** Develops and maintains the justice sector's IT architecture and central systems, aligned with Law 15-03.
- **IT Applications:** Designs and monitors software for digital case management, legal archiving, and e-filing platforms.
- **Information Systems Security:** Implements cybersecurity frameworks, conducts audits, and coordinates risk mitigation strategies in line with national standards.

B. Directorate of Foresight and Organization

This department addresses the structural, procedural, and methodological dimensions of justice reform. It ensures that modernization is not only technical but also systemic.

Key responsibilities include:

- Designing judicial organizational structures based on regional and international benchmarks.
- Conducting continuous evaluations of public justice services.
- Rationalizing operational procedures to improve efficiency and reduce costs.
- Developing standardized formats, procedural documentation, and curricula for training.

Sub-directorates:

- **Foresight:** Focuses on system-level planning, data analysis, and strategic recommendations for modernization and efficiency.
- **Organization:** Conducts audits, performs comparative assessments, and supports the reform oversight body in aligning practices with global standards.

1.3 Strategic Role in GRC Implementation

Despite the absence of a formal GRC framework, both directorates demonstrate embedded governance mechanisms through their mandates, risk oversight functions, and internal control structures. The ITC Directorate acts as the operational anchor for cyber resilience and risk management, while the Foresight and Organization Directorate plays a governance role in institutional design and procedural oversight. However, the coordination and alignment between the two remains a critical area for improvement.

The ACADYC-based diagnosis highlights both the strengths and gaps in current practices:

- Strengths include a strong mandate for modernization, centralized digital infrastructure, and emerging cybersecurity protocols.
- Gaps involve limited cross-functional coordination, fragmented risk communication, and lack of a unified compliance culture.

These insights offer a baseline for identifying strategic leverage points where GRC principles can be formally structured and institutionalized, thus enhancing accountability, boosting technology acceptance, and reinforcing digital trust across the Ministry of Justice.

2. GRC Diagnosis via ACADYC-inspired Approach

2.1 Introduction to Diagnosis

This subsection presents the core diagnosis of Governance, Risk Management, and Compliance (GRC) practices within the Directorate of Modernization. The Directorate currently lacks an explicit, integrated GRC framework. Instead, it operates with a collection of fragmented governance, risk, and compliance mechanisms. This diagnostic exercise aims to assess these practices holistically to identify strengths, gaps, and latent opportunities for integration.

The diagnostic strategy follows an ACADYC-inspired approach and relies on a three-pronged data collection method:

- Document Analysis to identify formal structures and mandates;
- Observation to capture organizational behaviors and cultural indicators;
- Conversational Interviews to uncover perceived risks, workarounds, and informal routines.

The purpose of this diagnostic phase is to develop a clear snapshot of how GRC is enacted—both formally and informally, within the Directorate. This includes:

- Formal Practices: Policies, legal instruments (e.g., Law 15-03), assigned roles, and system structures.
- Informal Practices: Cultural norms, communication patterns, behavioral adaptations, and leadership dynamics that shape how formal structures are interpreted and applied.

This nuanced diagnosis provides the foundation for designing a tailored GRC framework that aligns with the Ministry's digital transformation imperatives and organizational realities

2.2 Document-Based Diagnosis: Understanding the Formal and Informal GRC Landscape

To grasp how Governance, Risk Management, and Compliance (GRC) are operationalized within the Directorate of Modernization, this section analyzes a range of official documents. These include Executive Decrees (02-410 and 04-333), the Ministry's organizational chart,

Law 15-03 on the Modernization of Justice, the sector's digital transformation strategy, and progress reports.

This analysis sheds light on both the **formal GRC structures** designed on paper and the **informal practices** inferred from how policies and laws are likely interpreted, implemented, or bypassed in day-to-day realities.

A. Formal GRC Practices

Governance

- **Strategic Intent**: Law 15-03 and accompanying decrees articulate a clear ambition to modernize the justice sector. Reform is steered by top-level entities such as the National Committee for Justice Reform and a dedicated revitalization committee.
- **Dedicated Governance Structure**: The Directorate of Modernization operates directly under the Minister, reflecting its strategic centrality. It's functionally divided into sub-directorates for organization, IT systems, applications, and infrastructure.
- **Policy and Legal Foundation**: Law 15-03 lays out policies on digital justice components—like centralized IT governance (Art. 2), electronic communication and signatures (Art. 4–10), and videoconferencing (Art. 14–16). The Ministry is designated the national Certifying Authority for electronic signatures, institutionalizing its regulatory authority over digital trust systems.
- **Alignment with National Strategy**: The justice sector's roadmap is nested within Algeria's broader National Digital Transformation Strategy 2025–2030. The High Commission for Digitalization coordinated workshops to align sectoral portfolios with national priorities, suggesting a participatory governance model at the strategic level.

Risk Management

- **Security and Integrity**: Technical and legal protections for data, communications, and identity verification are mandated (Art. 3–10). Confidentiality and fidelity are central to digital court procedures such as videoconferencing.
- **Cyber Risk Legal Framework**: Broader legislative instruments—like Law 09-04 on cybercrime and Law 18-07 on personal data protection—complement Law 15-03, forming a national foundation for ICT risk regulation.

- **Accountability**: Legal liability is assigned to the Ministry for issued certificates (Art. 8), anchoring formal accountability into digital transactions.

Compliance

- **Benchmarking to Law 15-03**: This law remains the cornerstone of procedural and digital modernization, setting expectations for systems, processes, and ethical boundaries.
- **Electronic Procedure Adherence**: Specific articles (Art. 9–10, 14–16) define compliance protocols for digital communication and virtual court sessions, including secure documentation and recording requirements.
- **International Standards**: The Ministry's strategic documents repeatedly reference global benchmarks, implying an orientation toward compliance with international norms in judicial digitalization.

B. Inferred Informal GRC Practices

While documents articulate formal rules, they also leave space to infer how things might actually work on the ground. These gaps and ambiguities offer insight into informal dynamics that complement—or in some cases override—official frameworks.

- **Implementation Friction**: Although Law 15-03 outlines an ambitious vision, documents suggest that past efforts (e.g., the e-Algeria 2013 initiative) encountered delays. This signals the likely emergence of informal workarounds to keep progress alive amid limited capacities or misaligned expectations.
- **Discretion in Interpretation**: Vague phrases like “in the interest of the good administration of justice” (Art. 14) leave room for subjective application, enabling staff to adjust protocols based on local needs, leadership preferences, or practical constraints.
- **Power and Prioritization**: Although the Directorate’s role is formalized, the actual influence over resource allocation and project pacing may depend on its internal advocacy strength and informal negotiation with other departments like Finance or Judicial Affairs.
- **Cross-functional Collaboration**: The National Digital Transformation Strategy references inter-ministerial workshops and participatory design. These collaborative

practices, though not regulated, reflect a culture of informal coordination to navigate complexity and align competing interests.

- **Adaptive Learning**: Documents implicitly acknowledge that formal plans often evolve through "learning by doing." This points to a culture of improvisation, localized decision-making, and bottom-up problem-solving that shapes GRC enactment in real time.

2.3 Observation-Based Diagnosis: Uncovering GRC in Action

This subsection draws from observations made within the Directorate of Modernization, focusing on visible behaviors, team dynamics, and leadership practices that shape how governance, risk, and compliance actually unfold in daily operations. While technical dashboards or live systems could not be accessed, the researcher's field notes offer rich insight into the working atmosphere and informal cues that formal documents cannot capture.

The goal here is to move beyond static policy and examine the organizational "lived reality",how GRC elements are enacted, adapted, and sometimes bypassed in response to real-time demands and human behavior.

A. Formal GRC Practices (As Observed in the Field)

- **Operational Continuity**: Staff were consistently observed carrying out their assigned tasks within the formal chain of command, indicating that the foundational governance structure is functioning and respected in practice.
- **Security Protocols in Place**: Physical security controls—such as restricted access areas and authentication checkpoints—were visibly enforced, confirming that key formal risk mitigation mechanisms are active on-site.
- **Visible Modernization Efforts**: The deployment of core components of the justice digitalization strategy is evident, including:
    - The establishment of a primary data center and a backup IT site
    - Use of biometric identity verification
    - Video surveillance systems

- Videoconferencing for remote hearings and penitentiary institutions These visible assets reflect direct alignment with Law 15-03 and other modernization mandates.

- **Structured Project Implementation**: Staff work patterns and planning boards suggest adherence to pre-defined project timelines and goals, signaling the presence of a coordinated modernization process—even if informal influences coexist.

B. **Informal GRC Practices (Inferred from Organizational Behavior)**

While formal structures are functioning, much of what keeps the system running smoothly appears to lie in unwritten norms, collegial cooperation, and adaptive habits. The Directorate demonstrates a complex interplay of informal practices that either reinforce or substitute formal GRC mechanisms.

Informal Governance Dynamics

- **Collegial Decision-Making**: Rather than rigid hierarchy, many operational decisions seem to emerge through consensus and teamwork. Staff often consult one another before moving forward, creating a more collaborative governance layer.
- **Direct Access to Leadership**: Managers and directors maintain open channels with front-line staff, sometimes bypassing bureaucratic steps to accelerate problem-solving. This flattening of hierarchy creates a sense of agility and responsiveness.
- **Adaptive Leadership Style**: Leaders were observed prioritizing outcomes over procedures. Their flexibility fosters a pragmatic governance culture, especially when unexpected challenges arise.
- **Peer Support Culture**: Staff readily assist each other—technically and procedurally—without formal delegation. This informal solidarity plays a key role in maintaining momentum when formal instructions are delayed or unclear.
- **Fluid Knowledge Sharing**: Cross-disciplinary knowledge (technical, legal, operational) flows informally between staff, enriching team capacity and reducing dependency on rigid training pathways.

Informal Risk Management Practices

- **Peer Monitoring and Accountability**: Colleagues organically monitor each other's behaviors, especially concerning physical and digital security—creating an informal "watchdog" environment that supplements formal controls.
- **Creative Workarounds**: In the face of bureaucratic delays or technical obstacles, staff often devise improvised solutions that maintain output while respecting, as much as possible, the original intent of risk policies.
- **Experience-Based Risk Assessment**: Instead of strictly following risk registers or checklists, employees rely on professional judgment to balance speed, accuracy, and security.

  Shared Vigilance Culture: The team demonstrates a high level of collective sensitivity to risks—even in the absence of formal processes. Risks are often flagged informally and escalated quickly within the team.
- **Security Awareness in Practice**: While security procedures are formally emphasized, individual awareness varies. Some riskier practices (e.g., unprotected USB use or unlocked terminals) persist, indicating gaps between policy and day-to-day caution.

Informal Compliance Behaviors

- **Situational Flexibility**: Staff sometimes adjust formal procedures to accommodate workflow pressures, seeking practical solutions that respect compliance goals even if not strictly by the book.
- **Social Norm Reinforcement**: Compliance behaviors are often maintained not through audits or penalties, but through internalized team norms and mutual reminders,"how we do things here."
- **Feasibility-Based Interpretation**: Formal rules are interpreted with an eye toward what is realistically doable, especially when resource or time constraints make literal adherence impractical.
- **Cultural Internalization of Values**: Beyond what the law requires, the culture itself seems to promote respect for data confidentiality and procedural integrity, reinforcng compliance as a shared value rather than a top-down imposition.

This rich set of observations confirms that informal mechanisms play a critical role in how GRC practices evolve and are sustained within the Directorate. These insights will be instrumental in shaping an action plan that builds not only on legal mandates, but also on the tacit norms, human interactions, and adaptive intelligence already present within the institution.

2.4 Conversational Interviews-Based Diagnosis: Humanizing GRC from Within

This final diagnostic lens draws upon qualitative insights obtained through conversational interviews with staff members from various hierarchical levels within the Directorate. These dialogues provided not only confirmation of certain formal GRC mechanisms but also exposed the deep influence of culture, behavior, and peer dynamics on how governance, risk, and compliance are actually practiced.

The findings presented here reinforce earlier observations and document analyses, adding a human-centered dimension that reflects lived organizational realities, tensions, and adaptive intelligence within the Ministry's modernization journey.

A. Formal GRC Practices (As Reported by Personnel)

- Interviews consistently confirmed the existence of structured GRC practices aligned with legal and strategic frameworks, while also offering nuance on their practical application.
- **Strategic Orientation and Coordination**: Staff affirmed the presence of a clearly articulated digital transformation vision aligned with the National Digital Transformation Strategy 2025–2030 and presidential directives. The General Directorate for Modernization was widely acknowledged as the central hub coordinating this effort.
- **Formal Organizational Roles**: The interviews revealed that the structure outlined in formal documents is not only present on paper but functionally operational. Of particular note was the official appointment of a Responsable de la Sécurité des Systèmes d'Information (RSSI), responsible for cybersecurity strategy and oversight.
- **Capacity Building and Training**: Respondents cited ongoing formal training sessions led by the RSSI and other senior figures, emphasizing the Ministry's commitment to ensuring digital system readiness and developing internal capacities.

- **Institutional Collaboration**: Formal collaborations, especially with the **High Commission for Digitalization**, were highlighted as essential mechanisms to synchronize sectoral efforts with the national digital agenda.

Formal Risk Management Measures:

- **Security Protocols**: Interviewees acknowledged the presence of detailed procedures governing system access, data handling, and incident response. However, the degree of enforcement varied across departments.
- **Human Risk Focus**: The RSSI's explicit recognition of human error—especially with USB usage—was underscored, reflecting a shift toward behavioral risk awareness.
- **Systematic Risk Assessments**: Although formal risk assessments are conducted, there is variability in their consistency and methodological rigor.
- **Technical Risk Control**: Processes for vulnerability management and disaster recovery were confirmed to be in place, albeit challenged at times by staffing and budget constraints.

Formal Compliance Structures:

- Interviewees confirmed adherence efforts to the Law 15-03 and related legislation, recognizing its centrality in guiding digital modernization.
- Plans to integrate internationally recognized compliance frameworks were also mentioned as part of future strategic enhancements.
- Formal audit procedures**,** documentation protocols, and regulatory reporting mechanisms were acknowledged, even if their execution is sometimes impacted by workload and resource availability.

B. Informal GRC Practices (Emerging from Conversation)

The most illuminating aspects of the interviews lay in the realm of informal practices—those human-centered adjustments, interpretations, and social mechanisms that often make or break the success of formal systems.

Informal Governance Patterns

- **Collaborative Culture**: Staff unanimously described a highly collegial work culture where mutual aid is the norm. This informal support system often steps in when formal mechanisms stall.
- **Adaptive Leadership**: Leaders were praised for their flexible and responsive approach, often engaging directly with operational staff and encouraging practical problem-solving over strict adherence to hierarchy.
- **Hybrid Expertise**: A strong emphasis was placed on cross-functional competence—staff spoke of the informal value placed on developing both legal and technical literacy to bridge communication gaps.
- **Knowledge Circulation**: Expertise frequently flows through informal channels, such as peer discussions and mentoring, rather than through structured training.
- **Bottom-Up Decision Influence**: While formal structures remain intact, many decisions are shaped by feedback loops across ranks, enabling a form of participatory governance that is more dynamic than the formal chart implies.

Informal Risk Management Practices

- **Variable Security Awareness**: Interviewees acknowledged disparities in how seriously security protocols are taken, especially around USB use and data protection. Peer concerns reflect uneven behavioral implementation.
- **Workarounds as Survival Mechanism**: In the face of system constraints or inefficiencies, staff frequently reported resorting to informal workarounds,a pragmatic, if risky, method to keep operations flowing.
- **Peer Surveillance**: Security vigilance often comes from colleagues who casually monitor each other's actions—an informal yet effective layer of risk mitigation.
- **Diverging Risk Perceptions**: Differences emerged in how risks are perceived, with technical staff more attuned to cybersecurity threats, while administrative staff tend to prioritize operational fluidity.
- **Judgment-Based Decisions**: Risk decisions are frequently based on experience and intuition rather than adherence to structured frameworks, reflecting the real-world pressures of public sector environments.

Informal Compliance Dynamics

- **Real-World Interpretation of Rules**: Compliance is often adapted to match operational feasibility. Staff try to maintain alignment with the "spirit" of the law, even when procedural compliance proves difficult.
- **Peer-Driven Enforcement**: Compliance behaviors are shaped more by collective expectations than by top-down enforcement. Peer pressure and cultural norms often act as invisible enforcers of conduct.
- **Culture as a Compliance Anchor**: Values like confidentiality, integrity, and service to the citizen appear embedded in the culture and not just written in statutes.
- **Informal Learning and Reliance on Colleagues**: Not all staff feel confident in their understanding of compliance procedures, and many rely on experienced colleagues as informal advisors rather than consulting formal documentation.
- This interview-based diagnosis affirms that beyond laws, structures, and strategies, it is the people, their beliefs, judgments, shortcuts, and shared norms, who truly operationalize GRC on the ground. These insights will play a central role in tailoring the upcoming action plan, ensuring it is not only technically sound but also human-centered and realistically executable.

2.5 Synthesis of Diagnosis: Toward an Integrated Understanding of GRC Practices

This synthesis consolidates insights derived from the triangulation of three complementary diagnostic lenses—document analysis, in-situ observation, and conversational interviews. The goal is to construct a holistic picture of governance, risk management, and compliance (GRC) practices within the Directorate of Modernization. This multi-method approach highlights both formal structures and informal dynamics, revealing areas of alignment, friction, and latent potential.

2.5.1 Governance Practices: Formal and Informal

Formal Strengths

- The Directorate operates under a clear strategic framework, anchored in *Law 15-03* and aligned with the *National Digital Transformation Strategy 2025–2030*.

- Its organizational structure is well-defined, with mandates clearly distributed across specialized sub-directorates and direct oversight by the Minister of Justice.
- Formal governance instruments—policies, procedures, and training initiatives—are in place for key components such as centralized IT systems, digital communications, and the legal use of electronic signatures.
- Institutional collaborations, such as with the *High Commission for Digitalization*, reinforce alignment with national modernization goals.

Informal Strengths

- A pronounced collegial culture supports fluid knowledge sharing, collective engagement, and informal problem-solving.
- The leadership style is consistently described as agile and approachable, often bridging gaps between strategic intent and frontline realities.
- Staff members demonstrate hybrid skill sets—integrating legal and technical fluency—that enable more nuanced understanding and decision-making.
- Governance decisions are often made through participatory mechanisms, supplementing the rigidity of formal hierarchies.

Gaps and Frictions

- A misalignment may exist between strategic design and operational execution due to resource limitations and uneven levels of engagement.
- Informal workarounds, while efficient, risk bypassing formal governance safeguards.
- Governance consistency across initiatives and units remains a challenge, particularly in scaling best practices.

2.5.2 Risk Management Practices: Formal and Informal

Formal Strengths

- Legal and regulatory foundations emphasize the protection of data integrity, confidentiality, and system availability.
- A designated *Responsable de la Sécurité des Systèmes d'Information (RSSI)* leads structured risk management processes.

- Established protocols exist for access control, incident response, and technical safeguards such as biometric systems and IT backup facilities.
- Training initiatives are regularly conducted to raise awareness and ensure compliance with security protocols.

Informal Strengths

- Peer vigilance and a strong culture of shared responsibility contribute to a distributed, human-centric layer of security.
- Staff often conduct tacit, experience-based risk assessments in real-time, enhancing the responsiveness of risk controls.
- Adaptive behaviors allow teams to preserve operational flow when formal systems are slow or overly rigid.

Gaps and Frictions

- Security awareness levels vary significantly among staff, particularly concerning behaviors like USB handling.
- Informal workarounds may compromise formal controls and introduce vulnerabilities.
- Formal risk assessments and vulnerability management practices suffer from inconsistent application and insufficient resourcing.
- Translating security policy into sustainable behavior remains a key implementation challenge.

2.5.3 Compliance Practices: Formal and Informal

Formal Strengths

- The Directorate adheres to a clear legal framework for compliance, including *Law 15-03* and standards for digital identity and communication.
- Documentation, audit procedures, and compliance reporting are formally institutionalized.
- There are explicit plans to adopt internationally recognized compliance frameworks to enhance maturity.

Informal Strengths

- Cultural norms and peer expectations act as implicit enforcement mechanisms, reinforcing compliance behaviors.
- Staff tend to pragmatically interpret compliance requirements, striving to meet their underlying intent when literal adherence is difficult.
- Informal cooperation helps fill gaps in compliance knowledge, particularly in the absence of exhaustive procedural training.

Gaps and Frictions

- Uneven awareness of specific compliance requirements leads to inconsistencies in implementation.
- Resource constraints limit the frequency and depth of compliance monitoring.
- Staff often experience tension between achieving compliance and maintaining workflow efficiency.
- There is a perceptual divide between technical and administrative staff in terms of what constitutes high-priority compliance.

2.5.4 Key Integrative Insights

➢ **Complementarity of Formal and Informal Practices**

The Directorate's success in navigating its digital transition stems from the coexistence of formal structures and adaptive informal practices. The interaction between codified governance and social dynamics provides both stability and agility.

➢ **Human Factors as a Double-Edged Sword**

Personnel behaviors simultaneously enhance and threaten system resilience. While peer vigilance and collective responsibility are strengths, inconsistent practices around data handling underscore vulnerabilities.

➢ **Cultural Assets as Enablers**

The embedded culture of collegiality, agile leadership, and hybrid skill development offers fertile ground for further institutionalizing GRC, even in the absence of a unified framework.

- **Adaptation as a Strategy**

Rather than rigid implementation of directives, the Directorate relies on iterative adaptation, allowing it to maintain momentum despite institutional inertia or resource limitations.

- **Strategic-Operational Alignment**

The Directorate achieves vertical coherence by balancing strategic commitments with ground-level flexibility, essential in contexts of administrative complexity and evolving digital threats.

- **Knowledge as a Crosscutting Enabler**

The ability to merge legal and technical domains enhances the organization's capacity to meet both governance and compliance demands. This hybrid competence is a strategic advantage.

- **Collaborative Security and Compliance**

Informal problem-solving and shared vigilance create a robust support system that strengthens formal control mechanisms and facilitates early detection of issues.

- **Persistent Implementation Gaps**

Despite robust legal foundations and cultural strengths, the Directorate still grapples with uneven practices, capacity limitations, and inconsistencies that may hinder the full realization of its modernization ambitions.

2.5.5 GRC, Technology Acceptance, and Cyber Resilience

This section discusses how the diagnostic findings illuminate the potential of GRC frameworks to influence digital transformation outcomes. In particular, it analyzes how GRC practices—both formal and informal—affect technology acceptance, shape change management, and contribute to organizational cyber resilience. The analysis is anchored in the refined research questions, which seek to understand how GRC can serve not merely as a compliance mechanism but as a strategic enabler for navigating both human and technical challenges during digital transformation.

A. GRC Practices and Technology Acceptance

The case study findings underscore that existing GRC practices within the Directorate influence technology acceptance in multifaceted ways.

Facilitating Factors:

- A collegial work environment and culture of mutual support reduce resistance to adopting new tools.
- Hybrid skill sets—particularly legal-technical fluency—improve comprehension and perceived relevance of new digital systems.
- Agile leadership and flat communication hierarchies promote feedback loops, aligning digital tools with operational needs.
- Structured training by the RSSI builds user confidence and capability, reinforcing perceived ease of use and usefulness—two key constructs of the Technology Acceptance Model (TAM).

Barriers:

- Inconsistent levels of security awareness hinder unified engagement with system features.
- Resource constraints limit comprehensive user support, particularly in early stages of implementation.
- Compliance-related knowledge gaps may cause uncertainty, undermining trust in new systems.
- A disconnect between strategic plans and operational realities risks introducing solutions that don't fully reflect frontline needs.

Implications: A GRC framework adapted to this context should integrate operational feedback mechanisms, provide user-centric compliance guidelines, and embed technology acceptance metrics within risk assessment processes. Training must be dual-purpose: building technical skill and reinforcing the rationale for secure and compliant behaviors.

B. GRC Practices and Change Management

The case also sheds light on how governance, risk, and compliance elements influence change management—a critical pillar of digital transformation.

Strengths:

- National legal frameworks (e.g., Law 15-03) and internal strategic alignment foster a shared vision for change.

- Specialized directorates define clear roles, minimizing ambiguity.
- Adaptive leadership supports iterative change, allowing quick pivots.
- Bottom-up decision-making mechanisms increase stakeholder engagement, aligning with Kotter's model of leading change.

Weaknesses:

- Risk management remains uneven across units, weakening anticipation of change resistance or disruption.
- Gaps in compliance knowledge make transitions fragile.
- Informal workarounds—though efficient—can bypass structured change procedures.

Implications: An integrated GRC framework should formalize change-readiness assessments, build cross-functional change champions, and balance flexibility with process integrity. Compliance rollout should be phased and include feedback checkpoints to refine approaches in real time.

C. GRC Practices and Cyber Resilience

Cyber resilience emerges not just from technical robustness but from cultural and procedural adaptability—dimensions strongly shaped by GRC.

Enhancers of Resilience:

- Formal systems for backup, biometric authentication, and protocol enforcement provide technical baselines.
- Informal vigilance and peer-led security norms reinforce real-time protection.
- The RSSI's focus on human factors is a noteworthy alignment with ISO 27001, which now emphasizes personnel awareness and behavior.

Resilience Gaps:

- Security gaps arise from uneven application of formal policies.
- Informal workarounds, though operationally useful, may bypass control points.
- Limited resourcing delays remediation of known vulnerabilities.

Implications: Cyber resilience should be explicitly embedded within the GRC framework. This includes recurrent stress-testing of controls, cultural audits of security behavior, and enhanced support for secure improvisation, encouraging adaptive rather than rule-breaking responses to operational constraints.

2.6 ACTION PLAN: Toward an Integrated GRC Framework

The Directorate does not currently operate under a formalized, integrated GRC architecture, but many foundational elements already exist,To enhance its transformative potential, a tailored GRC framework should:

- Leverage Cultural Capital: Institutionalize strengths such as peer learning, agile leadership, and hybrid legal-technical skills.
- Address Critical Gaps: Target inconsistencies in compliance understanding, security awareness, and application of risk methodologies.
- Link the Three Pillars: Create structured interfaces between governance, risk, and compliance to harmonize processes.
- Embed Adaptive Feedback: Build in mechanisms that allow policy and practice to evolve with organizational learning.
- Balance Structure and Responsiveness: Provide just enough formalism to ensure reliability without stifling the informal dynamics that drive resilience and adoption.

Such a framework would transform GRC from a reactive, control-oriented system into a proactive enabler of successful, secure, and human-centered digital transformation.

Executive Summary

This action plan outlines a structured and context-sensitive roadmap for deploying a Governance, Risk Management, and Compliance (GRC) framework within the Directorate of Modernization of the Algerian Ministry of Justice. Anchored in the seven-phase ACADYC methodology, the plan directly addresses the human and technical obstacles revealed during the diagnostic phase.

The strategic intent is to operationalize GRC not merely as a compliance mechanism but as a strategic enabler of digital transformation. Through this plan, the Ministry will:

- Consolidate governance efforts into a coherent framework
- Strengthen risk management, especially on the human side
- Ensure systematic legal and regulatory compliance
- Harmonize governance, risk, and compliance functions
- Embed iterative feedback mechanisms linking policy with practice

- Cultivate internal capacity for resilience through hybrid skillsets and a collaborative culture

The full implementation spans 24 months, segmented into specific deliverables, timelines, and success criteria for each phase.

Phase 1: Initialization (1–2 Months)

Objectives:

- Define project scope, goals, and expected benefits
- Mobilize leadership and secure needed resources
- Establish project governance and designate stakeholders
- Initiate a project-specific risk management protocol

Key Activities:

- Scope definition and KPI selection
- Preparation and validation of a business case
- Constitution of the steering committee
- Mapping of stakeholder influence and expectations
- Formulation of a risk mitigation approach for project execution

Deliverables:

- Project charter and stakeholder map
- Resource plan and risk register
- Initial communication and project calendar

Success Indicators:

- Ministerial-level approval and commitment
- Functional implementation team
- Risk and stakeholder frameworks fully operational

Phase 2: Strategic Communication Plan (1 Month)

Objectives:

- Build buy-in through targeted messaging

- Anticipate and address resistance points
- Foster an informed and engaged ecosystem

Key Activities:

- Stakeholder segmentation and message tailoring
- Communication calendar and responsibility matrix
- Development of awareness, training, and feedback tools

Deliverables:

- Complete communication strategy and materials
- Feedback tools (surveys, channels, review protocols)

Success Indicators:

- Communication plan endorsement
- Activation of engagement tools and channels
- Measurable improvement in stakeholder understanding

Phase 3: IT Systems Analysis (2–3 Months)

Objectives:

- Assess the Ministry's current IT landscape
- Identify system interdependencies and vulnerabilities
- Align IT capabilities with GRC needs

Key Activities:

- IT asset inventory
- Visualization of data flows and architecture
- Governance audit of IT functions and ongoing digital initiatives

Deliverables:

- IT architecture map and systems audit report
- Gap analysis and prioritized IT upgrade roadmap

Success Indicators:

- Complete mapping of systems and dependencies
- Documented IT strengths, weaknesses, and integration points

Phase 4: Business Process Mapping (2–3 Months)

Objectives:

- Analyze current business processes and governance mechanisms
- Surface informal GRC practices and latent risks
- Identify opportunities for redesign and harmonization

Key Activities:

- Organizational structure mapping
- Interviews with key actors
- Evaluation of process effectiveness and regulatory alignment

Deliverables:

- Business process documentation and maps
- Compliance analysis and improvement proposals

Success Indicators:

- Comprehensive view of operational processes
- Clarity around accountability and process ownership
- High-impact, actionable business process recommendations

Phase 5: Target Business Model Design (2–3 Months)

Objectives:

- Redesign key business processes with embedded GRC principles
- Define future-state roles, decision rights, and workflows
- Develop an impact-aware change management strategy

Key Activities:

- Design of future-state process flows

- Specification of GRC-related KPIs and controls
- Organizational impact and capability assessment

Deliverables:

- Target operating model with performance indicators
- Change strategy linked to behavioral and skills alignment

Success Indicators:

- Alignment with strategic vision
- Process redesigns tested for feasibility and acceptance
- Adoption metrics integrated into the model

Phase 6: Target IT Architecture Design (2–3 Months)

Objectives:

- Define technical enablers for the GRC framework
- Ensure data integrity, interoperability, and cyber protection
- Prepare a phased IT deployment roadmap

Key Activities:

- Selection of tools, platforms, and integration pathways
- Data governance definition
- Planning for system enhancements or replacements

Deliverables:

- Target IT blueprint and system design documents
- Integration and cybersecurity plans
- Procurement and implementation roadmap

Success Indicators:

- Tool readiness and systems alignment with GRC needs
- Feasible IT deployment sequence

Phase 7: Implementation and Continuous Improvement (12+ Months)

Objectives:

- Roll out the GRC framework
- Institutionalize continuous monitoring and learning
- Evaluate performance and embed resilience

Key Activities:

- Change deployment and training
- Performance tracking and iterative reviews
- Post-implementation assessment and scaling recommendations

Deliverables:

- Updated procedures, deployed systems, and user training
- KPI dashboards and improvement cycles

Success Indicators:

- Smooth transition and user adoption
- Operationalization of continuous improvement protocols
- Enhanced risk posture and compliance traceability

Governance Structure

Steering Committee:

- High-level oversight and strategic decision-making
- Includes Ministerial representation, departmental heads, and external advisors

Implementation Team:

- Cross-functional experts handling technical and organizational streams
- Responsible for execution, integration, and monitoring

GRC Working Groups:

- Dedicated clusters for governance, risk, and compliance components
- Translate strategy into operational design

Change Network:

- Embedded actors in departments to facilitate buy-in and relay feedback

Risk Management for Implementation

Key Risks:

- Leadership disengagement
- Change resistance
- Resource constraints
- Competing initiatives
- Technical hurdles
- Capability gaps
- Scope drift

Mitigation Measures:

- Proactive leadership engagement
- Embedded change management practices
- Phase-based resource planning
- Risk tracking dashboards and real-time adjustments

Critical Success Factors

- Political and managerial commitment
- Authentic stakeholder involvement
- Synergy between technical tools and human adaptability
- Realism in planning and resilience in execution
- Ongoing learning, feedback, and iteration mechanisms

Conclusion

By embracing the ACADYC framework, the Ministry of Justice has a pragmatic and scalable path toward institutionalizing GRC. When executed with focus and agility, this plan has the potential to position GRC as a core pillar of digital trust, risk-aware governance, and adaptive transformation.

Section 3: Discussion Towards a Strategic Synthesis of GRC in Digital Transformation

This section synthesizes and critically interprets the empirical findings from both the semi-structured expert interviews and the embedded case study conducted at the Directorate of Modernization within Algeria's Ministry of Justice. It aims to answer the central research question: How can Governance, Risk, and Compliance (GRC) frameworks support organizations in addressing both human and technical challenges during digital transformation? Through a layered analysis, we advance the argument that GRC, when strategically integrated and contextually adapted, serves not merely as a compliance mechanism but as a dual-purpose enabler: it facilitates change management and technology acceptance (human dimension), while also reinforcing cybersecurity and organizational resilience (technical dimension).

1 GRC as a Dual Bridge: Formal Structures and Informal Dynamics

Both expert insights and the case study underscore the necessity of moving beyond a rigid interpretation of GRC. The interplay between formal mechanisms (e.g., policies, control frameworks, ISO/NIST alignment) and informal dynamics (e.g., leadership behavior, peer influence, culture) emerged as a central theme. Human experts emphasized the importance of trust, peer support, and cultural alignment in shaping the success of formal GRC programs. AI-generated experts, while focused on structural optimization, provided complementary views on how automation and policy modularity can improve GRC responsiveness.

In the case study, success in implementation often correlated with "invisible enablers": informal practices that filled functional gaps left by rigid controls. For instance, while documented training protocols existed, informal peer-to-peer support networks were critical in fostering acceptance. Likewise, resilience was not only supported by compliance audits but by daily practices of vigilance and informal coordination. Thus, GRC effectiveness is a function of *formal/informal integration*, not merely policy quality.

These findings strongly align with the literature. (Shahim et al., 2012) strategic alignment model already emphasized the need to align governance with operational realities across IT and business domains. Our field evidence affirms that this model must be expanded to explicitly account for informal cultural forces that shape or obstruct that alignment. Similarly, Racz et al. (n.d.) highlighted the gap between integrated GRC models and real-

world operationalization—this research provides concrete empirical validation of that observation.

2 Addressing the Human Dimension: GRC and Change Management

One of the clearest outcomes from both data sources is that GRC can strategically mitigate human resistance to digital transformation. Through formal components such as training, role clarity, and communication strategies, GRC frameworks address the UTAUT/TAM variables of perceived usefulness and ease of use. However, these alone are insufficient. As shown in both the interviews and the Ministry case, informal mechanisms such as social proof, managerial empathy, and cultural framing significantly influence behavioral intention.

The concept of "Technological Capital" (TC) is particularly relevant here. Organizational GRC initiatives that supported upskilling, promoted e-government literacy, and adapted messaging to audience-specific concerns (e.g., "What's In It For Me") saw greater acceptance. In contrast, GRC programs that failed to account for context-specific human dynamics encountered latent resistance despite surface-level compliance.

This reinforces the propositions made (Magsamen-Conrad et al., 2022), who argue that awareness, social support, and perception of benefit are key to user acceptance. Our data validate this by showing how GRC frameworks can serve as the delivery system for these acceptance enablers when properly designed. The introduction of e-government literacy by the United Nations (2024) also finds practical relevance in the Ministry’s attempt to bridge digital gaps through informal peer-based training efforts.

3 Navigating the Technical Dimension: Cybersecurity and Resilience Through GRC

From a technical standpoint, the interviews and case study affirm that GRC is indispensable in operationalizing cybersecurity and resilience. Risk assessment, compliance with evolving international frameworks (e.g., ISO 27001, NIS2), and layered control systems (e.g., Defense in Depth) all fall under GRC's domain. However, static GRC frameworks were often seen as misaligned with the pace and complexity of cyber threats, especially in underfunded or bureaucratic environments.

Participants stressed the need for adaptive, anticipatory GRC structures. For example, real-time threat intelligence, red teaming, and AI-enhanced compliance monitoring were highlighted as forward-looking extensions of traditional GRC. The Ministry’s case

confirmed that even in resource-constrained contexts, low-cost adaptive strategies (e.g., informal risk-sharing, internal knowledge networks) could reinforce resilience when formal structures lagged.

These findings reinforce the work of (Altaleb & Rajnai, 2024; Canadian center for cybersecurity,2024, n.d.), who both warn that cybersecurity governance must evolve beyond static defenses. The emergence of Cybercrime-as-a-Service (CaaS) and Ransomware-as-a-Service (RaaS), also mentioned in the (*WEF_Global_Cybersecurity_Outlook_2025*, n.d.-b) report, echoes participants' concerns about needing real-time, scalable, and intelligence-driven GRC architectures. Thus, our study not only aligns with these insights but contextualizes them in a developing country reality.

4 Comparative Insights: Human vs. AI Experts and Case Reality

Human experts provided a nuanced understanding of the informal and cultural elements essential to change management, while AI experts excelled at mapping structured solutions and benchmarking against global standards. The synthesis of both provides a richer picture: AI alone lacks contextual sensitivity, while human insight alone may underplay structural efficiencies. Their combined application offers a hybrid intelligence that could redefine next-generation GRC practices.

The case study functioned as a grounding mechanism, validating theoretical propositions with real-world constraints. It revealed that while many best practices exist on paper, their translation into action depends on contextual adaptation, leadership, and iterative learning. This underscores the danger of over-standardizing GRC without room for localization.

This duality reflects and extends prior literature. (Rachmatika, 2019b) introduced the TAM-Governance Extension model, which emphasized trust and perceived risk. Our research refines this by showing how formal structural assurance must be accompanied by informal signals of trustworthiness, especially in hierarchical or low-trust institutional contexts. The comparative strengths of human vs. AI perspectives echo the calls by (McIntosh et al., 2023)and (Benita Urhobo, 2024) for synergistic AI-human governance solutions.

5 Reframing GRC: From Control Apparatus to Strategic Capability

The cumulative findings compel a reframing of GRC: from a reactive, control-centric apparatus to a proactive, integrative strategic capability. When embedded holistically, GRC frameworks facilitate:

- Cross-functional coordination between IT and management
- Empowerment through training and cultural engagement
- Real-time adaptability to cyber and regulatory shocks
- Continuous learning loops that align policy with lived reality

Such a reframing is particularly urgent in emerging economies where infrastructural and human capital limitations are profound. The Algerian case illustrates both the obstacles (e.g., resource fragmentation, resistance) and the latent strengths (e.g., informal leadership, commitment to modernization) that can be leveraged through tailored GRC strategies.

This directly responds to the gaps identified by (Kraus et al., 2021) and (Siahaan et al., 2023), who called for contextualized GRC frameworks rooted in institutional realities. The case affirms that theory must be translated into strategies that are not only scalable but socially embedded.

Conclusion: Toward a Contextualized and Integrative GRC Model

This discussion affirms that GRC frameworks, when approached as adaptable, socio-technical systems, can serve as powerful enablers of digital transformation. Their impact lies not only in compliance assurance but in their capacity to align formal policies with informal organizational realities, thereby bridging the human-technical divide. Future models of GRC must emphasize flexibility, contextual embedding, and hybrid intelligence to remain relevant in increasingly volatile digital landscapes.

The path forward involves institutionalizing this duality: reinforcing formal mechanisms while cultivating the informal capacities that render transformation not only possible but sustainable.

Conclusion

This thesis set out to investigate the strategic potential of Governance, Risk, and Compliance (GRC) frameworks in navigating the complex human and technical challenges inherent in digital transformation. Challenging the narrow perception of GRC as a purely regulatory tool, the study explored its capacity to act as a dual-function enabler: supporting technology acceptance and managing cyber risks, while fostering adaptability and resilience.

Grounded in an interpretivist paradigm and informed by a qualitative methodology, combining expert interviews (human and AI-simulated) with a case study at the Algerian Ministry of Justice, this research provided a deeply contextualized analysis of how GRC is enacted both formally and informally within organizations.

The integrated findings underscore several key insights. First, the effectiveness of GRC frameworks depends not solely on the presence of formal policies and structures but on their interaction with informal organizational dynamics such as leadership behavior, peer support, and cultural norms. Second, GRC influences technology acceptance not only through formal mechanisms like training and communication but also through social proof, trust-building, and adaptive learning, all vital in building what the study conceptualized as "Technological Capital." Third, the operationalization of cybersecurity and resilience requires a hybrid model: formal controls aligned with standards must be reinforced by informal vigilance, knowledge sharing, and context-specific improvisation.

Importantly, the study revealed the complementary value of human and AI expert perspectives: while human experts offer cultural depth and sensitivity, AI models provide scalable, structured knowledge, together forming a "hybrid intelligence" approach to next-generation GRC design.

The research concludes that GRC, when embedded as a context-sensitive, integrative system, becomes more than a compliance mechanism, it becomes a strategic capability. Its power lies in harmonizing formal governance with informal organizational life, enabling institutions to build trust, manage change, mitigate digital risks, and adapt effectively to uncertainty.

Implications for Theory and Practice

Theoretically, this thesis contributes to the literature by empirically validating the interplay between formal and informal GRC practices and extending existing models (for example: TAM, UTAUT, GRC Strategic Alignment) through a socio-technical lens. It also introduces

the concept of Technological Capital as a practical outcome of effective GRC implementation.

Practically, it offers actionable guidance: practitioners should tailor GRC to institutional realities, integrate human factors and technical controls holistically, foster informal support cultures, and adopt adaptive leadership. GRC strategies should be agile, inclusive, and attuned to context, especially in resource-constrained environments.

Limitations and Future Research

While the study provides a robust qualitative foundation, its single-case focus limits generalizability. Future research should expand to cross-sectoral comparative studies, develop quantitative measures of formal/informal GRC impact, and further explore the ethical integration of AI in GRC strategy. Longitudinal research could also track how the balance between formal and informal practices evolves across digital transformation phases.

Final Reflection

Digital transformation is not merely about deploying new technologies, it is about reshaping how organizations think, operate, and adapt. This thesis affirms that Governance, Risk, and Compliance frameworks, when contextually embedded and strategically activated, can serve as the backbone of this transformation. By bridging the human-technical divide, embracing hybrid intelligence, and rooting governance in both policy and practice, GRC becomes the connective tissue that enables resilient, trusted, and forward-looking digital organizations.

Bibliography

1. *A process model for integrated IT governance, risk, and compliance management*. (n.d.).
2. Adebayo Adeyinka Victor, Mubarak A Moronkunbi, Oyetunde Christian Oyedeji, Popoola Olusegun Victor, & Shodunke Ajani Samuel. (2024). The Role of IT Governance Risk and Compliance (IT GRC) in Modern Organizations. *International Journal of Latest Technology in Engineering Management & Applied Science*, *13*(6), 44–50. https://doi.org/10.51583/IJLTEMAS.2024.130607
3. Adedamola Oluokun, Adebimpe Bolatito Ige, & Maxwell Nana Ameyaw. (2024). Building cyber resilience in fintech through AI and GRC integration: An exploratory Study. *GSC Advanced Research and Reviews*, *20*(1), 228–237. https://doi.org/10.30574/gscarr.2024.20.1.0245
4. Adedamola Oluokun, Courage Idemudia, & Toluwalase Vanessa Iyelolu. (2024). Enhancing digital access and inclusion for SMEs in the financial services industry through Cybersecurity GRC: A pathway to safer digital ecosystems. *Computer Science & IT Research Journal*, *5*(7), 1576–1604. https://doi.org/10.51594/csitrj.v5i7.1277
5. Arribi, C., & Boutarfa, S. (2024). Digital Transformation: Opportunities and Challenges of Digitization in Algeria. *Digital Transformation*, *12*(01).
6. Benita Urhobo. (2024). Understanding the role of artificial intelligence in enhancing GRC practices in cybersecurity. *World Journal of Advanced Research and Reviews*, *22*(2), 269–274. https://doi.org/10.30574/wjarr.2024.22.2.1340
7. Canadian center for cybersecurity,2024. (n.d.). *National cyber threat assessment 2025–2026*.
8. Christie, J., & Geary, C. (2024a). Digital Darwinism: Surviving the New Age of Business Disruption. *Vikalpa: The Journal for Decision Makers*, *49*(3), Article 3. https://doi.org/10.1177/02560909241271644
9. Coccia, M. (2019). A theory of classification and evolution of technologies within a Generalised Darwinism. *Technology Analysis & Strategic Management*, *31*(5), 517–531. https://doi.org/10.1080/09537325.2018.1523385
10. Crotty, M. (2020). *The foundations of social research: Meaning and perspective in the research process* (1st ed.). Routledge. https://doi.org/10.4324/9781003115700
11. Deistler, N., & Rentrop, C. (2022). IT-Compliance in KMU – Experteninterviews zum Status quo. *Wirtschaftsinformatik & Management*, *14*(1), 10–19. https://doi.org/10.1365/s35764-021-00380-5
12. Denzin, N. K., & Lincoln, Y. S. (Eds.). (2018). *The SAGE handbook of qualitative research* (Fifth edition). SAGE.
13. Doeze Jager, S. B., Born, M. Ph., & Van Der Molen, H. T. (2022). The relationship between organizational trust, resistance to change and adaptive and proactive employees' agility in an unplanned and planned change context. *Applied Psychology*, *71*(2), 436–460. https://doi.org/10.1111/apps.12327
14. Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151
15. Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLOS ONE*, *15*(5), e0232076. https://doi.org/10.1371/journal.pone.0232076
16. Karthick, M. V. (2023). *Systematic Literature Review on GRC - A Study on Best Practices and Implementation Strategy in GRC*. *16*(4).

17. Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital Transformation: An Overview of the Current State of the Art of Research. *Sage Open*, *11*(3), 21582440211047576. https://doi.org/10.1177/21582440211047576
18. Magsamen-Conrad, K., Billotte Verhoff, C. C., & Dillon, J. M. (2022). Technology Acceptance Models. In E. Y. Ho, C. L. Bylund, & J. C. M. Van Weert (Eds.), *The International Encyclopedia of Health Communication* (1st ed., pp. 1–8). Wiley. https://doi.org/10.1002/9781119678816.iehc0776
19. Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in is Research. *Journal of Computer Information Systems*, *54*(1), 11–22. https://doi.org/10.1080/08874417.2013.11645667
20. McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Computers & Security*, *134*, 103424. https://doi.org/10.1016/j.cose.2023.103424
21. National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (No. NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018
22. Olorunyomi Stephen Joel, Adedoyin Tolulope Oyewole, Olusegun Gbenga Odunaiya, & Oluwatobi Timothy Soyombo. (2024). The impact of digital transformation on business development strategies: Trends, challenges, and opportunities analyzed. *World Journal of Advanced Research and Reviews*, *21*(3), 617–624. https://doi.org/10.30574/wjarr.2024.21.3.0706
23. Rachmatika, T. (2019a). Digital Era Paradox: Integrating Technology Acceptance Model with Governance Risk & Compliance to Reduced the Perceived Digital Risk. *ACMIT Proceedings*, *3*(1), Article 1. https://doi.org/10.33555/acmit.v3i1.47
24. Rebecca Pariela, E. P., & Suparno, S. (2024). Reconstruction of Corporate Governance Legal System with Governance, Risk Management, and Compliance (GRC) Approach. *Asian Journal of Social and Humanities*, *3*(2), 261–272. https://doi.org/10.59888/ajosh.v3i2.443
25. *Sereir El Hirtsi Hayet, an-in-depth-study-for-a-proposed-national-cyber-security-strategy-for-digital-economy-in-alegria*. (n.d.).
26. Shahim, A., Batenburg, R., & Vermunt, G. (2012). Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies. In M. D. Hercheui, D. Whitehouse, W. McIver, & J. Phahlamohlaka (Eds.), *ICT Critical Infrastructures and Society* (Vol. 386, pp. 202–212). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-33332-3_19
27. Siahaan, M., Suharman, H., Fitrijanti, T., & Umar, H. (2023). Will the integrated GRC implementation be effective against corruption? *Journal of Financial Crime*, *30*(1), 24–34. https://doi.org/10.1108/JFC-12-2021-0275
28. Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*, *22*, 960–967. https://doi.org/10.1016/j.promfg.2018.03.137
29. UNITED NATIONS 2024. (2024). *UNITED NATIONS E-GOVERNMENT SURVEY 2024: Accelerating digital transformation for... sustainable development - with the addendum on art*. UNITED NATIONS.
30. Venkatesh, Morris, Davis, & Davis. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540
31. Vergara Cobos. (2024). Cybersecurity Economics for Emerging Markets. *CYBERSECURI T Y*.
32. *WEF_Global_Cybersecurity_Outlook_2025*. (n.d.-a).
33. Yin, R. K. (2018). *Case study research and applications: Design and methods* (Sixth edition). SAGE.

Appendices

Appendix one:

Master's Thesis Interview Guide

Qualitative Research on Digital Transformation through the Lens of Governance, Risk, and Compliance (GRC)

Research Context:
This interview is part of a graduate thesis exploring the strategic alignment of Governance, Risk, and Compliance (GRC) with digital transformation processes in organizations. The goal is to gain expert insights on the institutional, cultural, and operational factors that influence technology acceptance and cyber resilience and how can GRC framework address them. Your responses will remain confidential and anonymized unless otherwise agreed.

SECTION A: ORGANIZATIONAL PRACTICES AND TECHNOLOGY ACCEPTANCE

- Based on your experience, what are the key factors that influence how well an organization adopts new technologies?
- Could you share an example where structured planning or leadership support helped reduce resistance to digital transformation?
- In your view, how do internal rules, communication strategies, or accountability systems affect the success of new digital initiatives? What challenges do organizations face in managing change when introducing new tools or platforms?

SECTION B: RISK THINKING AND CYBER RESILIENCE

- In the digital projects you've observed, what types of risks (technical, human, procedural) were most concerning?
- How do organizations you've worked with prepare for or respond to cybersecurity threats?
- Have you seen examples of strong internal practices (even if informal) that help build resilience against these risks?
- What role do leadership, training, or internal culture play in shaping an organization's response to digital threats?

SECTION C: STRATEGY, STRUCTURE, AND INSTITUTIONAL LEARNING

- What internal features (structure, leadership, rules) do you think support or hinder digital transformation efforts?
- From your perspective, do organizations with a proactive mindset toward risk and internal accountability perform better in digital projects? Why?
- In successful digital initiatives you've witnessed, what kinds of internal systems or habits made the difference?

- If you were to advise a government or company designing a system to guide and protect tech adoption, what core elements would you include (e.g., leadership support, role clarity, risk anticipation, structured decision-making)?

OPTIONAL REFLECTION: CONCEPTUAL FRAMING

- Some international frameworks refer to Governance, Risk, and Compliance (GRC) as key pillars of successful transformation. Based on your experience, do these ideas resonate in your context—even if under different names or forms? Why or why not?

Thank You

Your insights are invaluable to this research. Thank you for your time and for sharing your professional experience. Should you have any questions or wish to receive a summary of the findings, please do not hesitate to reach out.

Best regards.

Hadil Boulaliat

Phone number (WhatsApp):0

Emai1 : h