iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

CYBERSECURITY GOVERNANCE AND DATA PRIVACY IN CLOUD COMPUTING: AN INTEGRATED RISK AND COMPLIANCE FRAMEWORK FOR REGULATED ORGANIZATIONS

Rashid Hussain
Nour Internet Company for communication & IT, Riyadh, Saudi Arabia
corporate.lawyer.ksa@gmail.com
00966-566751233

ABSTRACT
Cloud computing has become a foundational component of digital transformation, but its distributed architecture, shared-responsibility model, extensive third-party dependencies and data-intensive operations create overlapping cybersecurity, privacy and regulatory risks. In many organizations, these risks are still governed through separate security, privacy, legal, compliance and vendor-management processes. Such fragmentation can produce inconsistent risk ownership, duplicated controls, weak visibility over cloud supply chains and gaps between technical incident response and regulatory obligations. This study examines how cybersecurity governance and data privacy can be integrated within cloud environments and develops a conceptual governance architecture for regulated organizations. The study uses a structured review and comparative framework analysis, with a historical evidence cutoff of 30 June 2024. It considers the NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001:2022, Saudi Arabia's Personal Data Protection Law and its implementing framework, the Saudi National Cybersecurity Authority's cloud and critical-systems controls, and the EU and UK GDPR regimes. The analysis identifies six recurring governance domains: governance and accountability; integrated risk assessment; data protection and privacy; cloud and third-party security; incident response and resilience; and assurance and continuous improvement. On this basis, the paper proposes the Integrated Cloud Cybersecurity and Privacy Governance Framework (ICCPGF). The framework is intended to help organizations map regulatory obligations to cybersecurity outcomes, assign accountable ownership and coordinate cloud, privacy and third-party risk management. The proposed framework is conceptual rather than empirically validated. Future research should test its applicability through case studies, practitioner surveys and maturity assessments in regulated and cloud-intensive sectors.

Keywords:
Cybersecurity Governance; Cloud Security; Data Privacy; Saudi PDPL; NIST CSF 2.0; ISO/IEC 27001; GDPR; GRC; Third-Party Risk Management; Cyber Resilience; Regulatory Compliance.

1. INTRODUCTION

Cloud computing changes both the technical architecture of information systems and the governance model through which risk is allocated. Data, applications and security functions may be distributed among customers, cloud service providers, managed service providers, software suppliers and other subcontractors. This creates dependencies that are difficult to manage through a security-only approach. A control can be technically effective while still failing to address privacy, contractual or regulatory obligations; conversely, a privacy policy can be legally sound while lacking operational mechanisms for monitoring, detection, recovery and assurance.

The governance challenge has become more prominent as cybersecurity frameworks increasingly emphasize enterprise-level accountability. NIST CSF 2.0, published on 26 February 2024, expanded the framework for organizations of all sizes and sectors and introduced GOVERN as a core function. NIST also increased emphasis on cybersecurity supply-chain risk and on integrating cybersecurity with enterprise risk management (Pascoe, Quinn, & Scarfone, 2024). In Saudi Arabia, the National Cybersecurity Authority (NCA) has established cybersecurity controls relevant to cloud service providers and cloud service tenants, while the Personal Data Protection Law (PDPL) establishes a parallel data-protection governance environment. International organizations may additionally be subject to the EU GDPR, UK GDPR and contractual or sector-specific obligations.

This paper argues that these requirements should not be treated as isolated compliance silos. It develops an integrated model in which cybersecurity, privacy, cloud, third-party and regulatory risks are governed through a

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

common architecture. The purpose is not to replace established standards or legislation, but to provide a practical governance layer through which their objectives can be coordinated.

1.1 Research Objectives and Questions

The study has four objectives: (1) identify the principal points of convergence between cybersecurity and privacy in cloud environments; (2) compare major governance themes across selected regulatory and standards frameworks; (3) identify governance gaps created by fragmented organizational approaches; and (4) propose an integrated conceptual framework.

RQ1: How do cybersecurity and data-privacy risks converge in cloud-computing environments?

RQ2: Which governance themes recur across NIST CSF 2.0, ISO/IEC 27001:2022, Saudi cybersecurity/privacy requirements, and EU/UK GDPR regimes?

RQ3: What governance gaps may arise when cloud, cybersecurity, privacy and third-party risks are managed separately?

RQ4: How can these requirements be organized into an integrated governance framework for regulated organizations?

2. LITERATURE AND REGULATORY CONTEXT

2.1 Cloud Computing and Shared Responsibility

Cloud adoption transfers some operational activities to service providers but does not eliminate organizational accountability. The distribution of responsibility varies by service model and contract. Consequently, organizations need explicit ownership for identity and access management, configuration, logging, encryption, data lifecycle management, incident coordination, supplier assurance and continuity. The NCA's Cloud Cybersecurity Controls (CCC-1:2020) were designed specifically to reduce cybersecurity risks for both cloud service providers (CSPs) and cloud service tenants (CSTs). The NCA described the 2020 controls as comprising 37 main controls and 96 subcontrols for CSPs, and 18 main controls and 26 subcontrols for CSTs (NCA, 2020).

2.2 Cybersecurity Governance

Cybersecurity governance connects technical security outcomes with organizational strategy, accountability and enterprise risk. NIST CSF 2.0 represents an important development because governance is explicitly incorporated as one of six functions: GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER. The framework does not prescribe a single implementation method; rather, it provides outcome-oriented guidance that organizations can adapt to sector, size and maturity. This makes it suitable as a governance backbone, but organizations still need to map its outcomes to legal, privacy, contractual and cloud-specific obligations.

2.3 Information Security Management

ISO/IEC 27001:2022 provides a management-system approach to information security based on risk assessment, leadership, planning, support, operation, performance evaluation and continual improvement. Its management-system logic is valuable for integrated governance because it treats security as an organizational process rather than a collection of isolated technical controls. In an integrated cloud governance model, ISO/IEC 27001 can therefore support assurance, auditability, risk treatment and continual improvement while other frameworks contribute more specific privacy or cloud requirements.

2.4 Privacy and Data Protection

Privacy governance introduces requirements that extend beyond confidentiality. Organizations must consider lawful and transparent processing, purpose limitation, data minimization, accuracy, retention, data-subject rights, accountability, breach management and cross-border transfers. The Saudi PDPL and its implementing framework establish data-protection obligations within the Kingdom, while the EU GDPR and UK GDPR provide mature accountability-based privacy regimes. For organizations operating across jurisdictions, privacy governance therefore needs to be connected to technical data inventories, cloud architecture, vendor management and incident-response processes.

2.5 Third-Party and Supply-Chain Risk

Cloud services are inherently dependent on external providers and layered supply chains. A regulated organization may have a direct contract with a CSP while the service itself depends on additional infrastructure, software, support and subprocessors. NIST CSF 2.0 gives greater prominence to supply-chain risk, while Saudi NCA controls include third-party and cloud-computing cybersecurity as an explicit governance area in critical-system controls. Integrated governance therefore requires due diligence before onboarding, contractual security/privacy obligations, ongoing monitoring, incident-notification requirements, exit planning and evidence of control effectiveness.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

2.6 From Perimeter Security to Cloud Governance

Traditional information-security models were often designed around organizational boundaries: systems, networks and data were assumed to reside primarily within infrastructure directly controlled by the enterprise. Cloud computing weakens that assumption. Infrastructure, platform and software services redistribute technical responsibility across providers and customers, while managed services, application programming interfaces, identity providers, content-delivery networks and subprocessors create additional dependencies. The governance problem is therefore not simply whether a particular control exists, but who is accountable for designing, operating, monitoring and evidencing that control.

This shift is especially important in regulated organizations because responsibility cannot necessarily be outsourced with the technical activity. A customer may rely on a cloud provider for physical security, virtualization, availability or managed security capabilities, yet still retain responsibilities for access governance, data classification, lawful processing, retention, supplier oversight and regulatory notification. The practical implication is that the shared-responsibility model must be translated into a shared-accountability map. That map should identify the control objective, the party operating the control, the party accountable for the outcome, the evidence required and the escalation path when the control fails.

Cloud governance should consequently be viewed as an enterprise-governance problem rather than an infrastructure-security problem. Business owners determine the purpose and criticality of processing; privacy and legal functions identify regulatory constraints; cybersecurity teams define protective and detective requirements; procurement and vendor-management teams translate requirements into contracts; and internal audit or assurance functions test whether the resulting arrangements operate as intended. ICCPGF is designed to connect these activities.

2.7 Cybersecurity Governance and Enterprise Risk Management

Cybersecurity governance is most effective when cyber risk is expressed in terms that can be understood within enterprise risk management. Technical findings such as vulnerable configurations, weak identity controls or incomplete logging become governance issues when they can affect service continuity, confidentiality, regulatory compliance, contractual commitments or strategic objectives. NIST CSF 2.0 reinforces this relationship by adding GOVERN to the framework's core and by positioning cybersecurity risk strategy, expectations and policy as organizational outcomes.

The governance function is particularly relevant to cloud environments because decisions concerning providers, architectures, data location, resilience and concentration risk are often made outside the security function. A mature governance model therefore needs defined risk appetite, decision rights, exception processes and escalation thresholds. It should also distinguish between risk ownership and control operation. A cloud engineering team may operate a technical control, for example, while a business owner remains accountable for accepting residual risk.

The integration proposed in this paper extends that logic to privacy and third-party risk. Rather than maintaining separate registers that describe the same cloud service from different perspectives, an organization can establish a linked risk record. Cybersecurity impact, personal-data exposure, contractual dependency, regulatory significance and resilience consequences can then be evaluated together while preserving specialist assessments where necessary.

2.8 Privacy Governance as an Operational Discipline

Privacy compliance is frequently documented through notices, policies, records of processing and contractual clauses. These are necessary governance instruments, but effective privacy protection also depends on operational controls. Data minimization depends on system design; retention depends on technical deletion capability; confidentiality depends on identity, access and encryption controls; breach assessment depends on reliable logs and incident triage; and data-subject rights depend on the organization's ability to locate and manage personal data across systems and suppliers.

This creates a strong dependency between privacy governance and information-security governance. The two disciplines are not identical: privacy addresses legitimate and appropriate processing of personal data, whereas cybersecurity has a broader concern with confidentiality, integrity, availability and resilience of information and systems. Nevertheless, they share important control mechanisms and evidence sources. The ICCPGF therefore treats privacy as a distinct governance domain that is operationally connected to security, cloud architecture and third-party management.

For multinational or cross-border organizations, the need for integration becomes stronger. Different privacy regimes may impose different legal tests, terminology and notification obligations, but the underlying organization still requires a reliable inventory of systems, data, processors, locations, access paths and retention periods. A

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

technically accurate data map can therefore become a common governance asset supporting privacy assessments, security risk analysis, incident response and supplier oversight.

2.9 Saudi Regulatory Context

Saudi Arabia's digital transformation has been accompanied by the development of national cybersecurity and data-protection requirements. The NCA's Cloud Cybersecurity Controls (CCC-1:2020) were explicitly developed for cloud service providers and cloud service tenants. The framework was intended to establish cybersecurity requirements for cloud services and improve readiness against cyber risks. This dual perspective is significant because it recognizes that secure cloud adoption requires controls on both sides of the service relationship.

The Saudi PDPL adds a complementary privacy-governance dimension. For organizations processing personal data, cloud decisions may therefore require consideration of both cybersecurity controls and data-protection obligations. The compliance task is not simply to maintain two checklists. A single cloud service can simultaneously raise questions concerning access control, data classification, processor governance, transfer arrangements, retention, incident response and evidence of compliance.

The ICCPGF is particularly suitable for this environment because it does not attempt to merge legal regimes into a single legal standard. Instead, it provides a governance architecture through which different obligations can be mapped to common operational processes while preserving their legal identity. This distinction is important: a cybersecurity control may support a privacy obligation without replacing it, and a contractual clause may allocate responsibility without eliminating regulatory accountability.

2.10 Third-Party and Cybersecurity Supply-Chain Risk

Modern cloud services depend on interconnected supply chains. A provider may use subprocessors, telecommunications providers, software components, identity platforms and specialist managed services. Consequently, a customer's risk exposure can extend beyond the entity with which it has a direct contract. NIST CSF 2.0 addresses cybersecurity supply-chain risk within GOVERN and includes outcomes concerning due diligence, contractual requirements, monitoring, incident participation and activities following termination of a supplier relationship.

A lifecycle approach is therefore preferable to a one-time vendor questionnaire. Before contracting, organizations should identify service criticality, data sensitivity, architectural dependencies and regulatory requirements. During contracting, risk decisions should be reflected in security schedules, audit or assurance mechanisms, incident-notification obligations, business-continuity commitments, subcontractor governance and exit provisions. During operation, the organization should monitor material changes, assurance reports, incidents, vulnerabilities and service performance. At termination, it should confirm data return or deletion, revoke access, preserve necessary records and manage transition risk.

This lifecycle is incorporated into ICCPGF because supplier risk is simultaneously a cybersecurity, privacy, resilience and legal issue. The framework encourages one coordinated third-party governance process with specialist inputs rather than disconnected reviews that may produce inconsistent requirements.

2.11 Incident Response, Privacy Breach Management and Resilience

Cloud incidents can move rapidly across organizational and jurisdictional boundaries. A security event may begin as an availability or credential issue and later be identified as unauthorized access to personal data. Effective response therefore requires both technical and governance pathways. Security operations need mechanisms for containment, evidence preservation and recovery, while privacy and legal teams need sufficient facts to assess notification obligations, contractual commitments and regulatory exposure.

An integrated incident model should establish predefined triggers for cross-functional escalation. Examples include suspected exposure of personal data, compromise of privileged cloud accounts, material service outage, ransomware, compromise of a critical supplier or evidence that data may have been transferred to an unauthorized location. The model should define who decides whether an incident is material, who communicates with regulators or customers, and how evidence is preserved.

Resilience extends beyond recovery from a single event. It includes the organization's capacity to anticipate dependencies, withstand disruption, restore critical services and learn from failures. Post-incident reviews should therefore feed into risk registers, supplier assessments, architecture standards, privacy assessments and control design. This closes the governance loop between RESPOND/RECOVER activities and continuous improvement.

2.12 Assurance, Metrics and Evidence

Integrated governance requires evidence. Policies and control descriptions alone cannot demonstrate that controls operate effectively. Organizations should identify evidence sources for each material control objective, including configuration records, access reviews, vulnerability-management reports, incident exercises, supplier assurance reports, privacy assessments, audit findings and management reviews.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Metrics should be selected carefully. Large numbers of operational measures can create the appearance of control without demonstrating risk reduction. A governance-oriented dashboard should combine leading and lagging indicators and connect them to risk appetite. Examples include percentage of critical cloud suppliers with current assurance evidence; overdue high-risk remediation actions; privileged-access review completion; mean time to escalate privacy-relevant incidents; percentage of high-risk processing activities with completed assessments; recovery-test success; and unresolved contractual security exceptions.
ICCPGF does not prescribe universal thresholds because organizational context matters. Instead, it proposes that metrics be traceable to governance objectives and reviewed by accountable owners. This allows management to distinguish between control activity and meaningful assurance.

3. METHODOLOGY

This study adopts a qualitative structured review and comparative framework-analysis methodology. The evidence base is intentionally bounded to regulatory instruments, standards, official guidance and relevant academic literature available up to 30 June 2024. This historical cutoff is used to preserve the integrity of the analysis and avoid attributing later regulatory developments to the earlier period.
The comparative analysis uses six coding domains derived iteratively from the selected frameworks: (1) governance and accountability; (2) integrated risk assessment; (3) data protection and privacy; (4) cloud and third-party security; (5) incident response and resilience; and (6) assurance and continuous improvement. Each source is examined for objectives, responsible actors, control orientation, risk treatment and evidence/assurance mechanisms. The approach is conceptual: it does not claim empirical measurement of control effectiveness or regulatory compliance.

4. COMPARATIVE FRAMEWORK ANALYSIS

Table 1 compares NIST CSF 2.0, ISO/IEC 27001:2022, the Saudi PDPL, the NCA Cloud Cybersecurity Controls (CCC-1:2020) and the EU/UK GDPR regimes across the six coding domains used in this study.

Framework	Governance	Risk	Privacy/ Data	Cloud/Third Party	Incident/ Resilience	Assurance
NIST CSF 2.0	Strong	Strong	Supporting	Strong supply-chain focus	Strong	Profiles/Tiers & outcomes
ISO/IEC 27001:2022	Strong	Strong	Security-oriented	Supplier/control context	Strong	Audit & continual improvement
Saudi PDPL	Accountability-focused	Privacy risk	Strong	Processor/transfer relevance	Breach/privacy response	Compliance evidence
NCA CCC-1:2020	Strong	Strong	Security/data controls	Very strong	Strong	Compliance monitoring
EU/UK GDPR	Strong accountability	Risk-based	Very strong	Processor/transfer governance	Breach obligations	Accountability/documentation

The comparison demonstrates that no single selected framework fully covers the combined governance problem. NIST CSF 2.0 provides a flexible cybersecurity-risk architecture; ISO/IEC 27001 provides a management-system and assurance mechanism; privacy legislation establishes legal accountability for personal-data processing; and NCA controls provide Saudi-specific cybersecurity requirements, including cloud and third-party considerations. Integration therefore depends on organizational mapping rather than selecting one framework as a universal substitute for the others.

5. PROPOSED INTEGRATED CLOUD CYBERSECURITY AND PRIVACY GOVERNANCE FRAMEWORK (ICCPGF)

5.1 Governance and Accountability

The first domain establishes senior-management oversight, policy ownership, risk appetite, regulatory mapping and clear lines of accountability. Cybersecurity, privacy, legal, compliance, cloud architecture, procurement and vendor management should operate under defined decision rights. The organization should maintain a consolidated obligation register linking regulatory requirements, contractual commitments and security objectives to accountable owners.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

5.2 Integrated Risk Assessment

The second domain combines cybersecurity, privacy, cloud, legal and third-party risks into a common assessment process. This does not require all risks to use identical scoring, but it requires common escalation criteria and an enterprise view of dependencies. High-risk cloud processing should consider threat likelihood, business impact, data sensitivity, concentration risk, cross-border exposure, supplier dependency and recovery requirements.

5.3 Data Protection and Privacy

The third domain embeds privacy into technical and operational governance. Core activities include data classification and inventories, purpose and lawful-basis documentation where applicable, minimization, retention, encryption, access controls, data-subject request processes, privacy-by-design reviews and cross-border transfer governance. Privacy obligations should be traceable to system owners and cloud architectures rather than maintained only as legal documentation.

5.4 Cloud and Third-Party Security

The fourth domain governs the extended enterprise. Due diligence should assess provider security posture, certifications, architecture, data location, subcontracting, incident capabilities, resilience and exit arrangements. Contracts should translate risk decisions into enforceable requirements covering security controls, audit/assurance rights, breach notification, confidentiality, subprocessors, business continuity, data return/deletion and regulatory cooperation.

5.5 Incident Response and Resilience

The fifth domain connects technical response with privacy and regulatory decision-making. Incident plans should define escalation from security operations to privacy, legal, communications and senior management. Organizations should maintain evidence needed to assess affected systems, personal data, jurisdictions, contractual notification requirements and recovery priorities. Exercises should test both technical containment and governance decision-making.

5.6 Assurance and Continuous Improvement

The final domain establishes control testing, internal audit, metrics, key risk indicators, management review and remediation. Assurance should cover both internal controls and third-party dependencies. Lessons from incidents, audits, regulatory change, threat intelligence and business transformation should feed back into policies, risk assessments and cloud architecture decisions.

6. Detailed ICCPGF Control Architecture

Table 2 elaborates each of the six ICCPGF domains introduced in Section 5 into representative objectives, primary owners, illustrative evidence and the framework themes each domain draws on, providing a practical reference for assigning accountability and evidence requirements.

Domain	Representative Objectives	Primary Owners	Evidence Examples	Related Framework Themes
Governance & Accountability	Risk appetite; policy; roles; obligation mapping; exceptions	Board/Executive; CISO; DPO/Privacy; Legal; Risk	Policies; committee minutes; risk acceptance; obligation register	NIST GOVERN; ISO leadership/planning; PDPL/GDPR accountability
Integrated Risk Assessment	Cyber, privacy, cloud, supplier and resilience risk evaluated together	Risk; Security; Privacy; Business owners	Risk assessments; DPIA/privacy assessments; architecture reviews	NIST IDENTIFY/GOVERN; ISO risk assessment
Data Protection & Privacy	Classification; minimization; retention; access; transfer governance	Privacy/DPO; Data owners; Security; Legal	Data inventory; retention schedule; access reviews; transfer records	PDPL; EU/UK GDPR; ISO security controls
Cloud & Third-Party Security	Due diligence; shared	Procurement; Vendor Risk;	Due diligence; contracts;	NCA CCC; NIST GV.SC; ISO supplier controls

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

	responsibility; contracts; monitoring; exit	Security; Legal; Cloud teams	SOC/ISO evidence; exit plans	
Incident Response & Resilience	Detection; escalation; breach assessment; recovery; exercises	SOC/CSIRT; Privacy; Legal; BCM; Communications	Incident records; playbooks; exercise reports; recovery tests	NIST DETECT/RESPOND/RECOVER; NCA resilience
Assurance & Improvement	Testing; audit; metrics; remediation; management review	Internal Audit; GRC; Control owners	Audit reports; KRIs/KPIs; remediation tracker; management review	ISO performance evaluation/improvement; NIST Profiles/Tiers

7. OPERATIONALIZING THE ICCPGF

Implementation can begin with an obligation-and-control mapping exercise. An organization first identifies applicable legal, regulatory, contractual and standards-based requirements. These requirements are then mapped to the six ICCPGF domains and to existing controls. Gaps are assigned owners, risk ratings and remediation dates. This approach avoids duplicating a control merely because several frameworks express the same underlying objective.

For example, supplier governance can simultaneously support NIST supply-chain outcomes, ISO/IEC 27001 supplier controls, NCA cloud requirements and privacy processor obligations. Similarly, an incident-response workflow can support detection and response objectives while also enabling legal assessment of breach-notification duties. The integrated model therefore seeks control reuse with explicit traceability, rather than compliance-by-checklist.

8. PRACTICAL IMPLEMENTATION ROADMAP

Phase 1 – Scope and obligation inventory: Identify regulated business services, cloud platforms, personal-data processing, critical suppliers and applicable legal/contractual obligations. Establish a single obligation register and nominate accountable owners.

Phase 2 – Current-state mapping: Map existing cybersecurity, privacy, cloud and vendor controls to the six ICCPGF domains. Record duplicate controls, missing evidence, inconsistent ownership and unaddressed dependencies.

Phase 3 – Risk integration: Link cyber, privacy, supplier and resilience assessments for the same service. Establish common escalation criteria while retaining specialist scoring where required.

Phase 4 – Control rationalization: Create a common control library. Where one control supports multiple obligations, preserve traceability to each source rather than operating duplicate processes.

Phase 5 – Contract and supplier alignment: Review critical supplier contracts against security, privacy, resilience, notification, audit, subcontracting and exit requirements. Prioritize gaps according to service criticality and data sensitivity.

Phase 6 – Incident integration: Create cross-functional triggers and decision trees connecting SOC/CSIRT activity with privacy, legal, business continuity and communications functions.

Phase 7 – Assurance and maturity review: Define evidence requirements, KRIs/KPIs, internal audit coverage and management review. Reassess maturity periodically and after material incidents, regulatory changes or architectural transformations.

9. DISCUSSION

The principal implication of the proposed framework is organizational rather than purely technical. Cloud security failures frequently cross functional boundaries: a misconfiguration can become a confidentiality incident; a vendor outage can become a resilience issue; an unauthorized disclosure can create privacy and contractual notification obligations; and inadequate supplier oversight can expose both security and compliance weaknesses. Treating these outcomes through separate governance channels can delay decisions and obscure ownership.

The Saudi context illustrates the value of integration. Organizations may need to align national cybersecurity controls with PDPL requirements while simultaneously using international standards for customer assurance or

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

operating across jurisdictions. A common governance architecture can support this multi-framework environment without suggesting that one framework legally replaces another. For cloud service providers in particular, the model can connect enterprise risk, service design, customer obligations, privacy governance, vendor dependencies and operational resilience.

The framework also supports a broader governance, risk and compliance (GRC) model. GRC platforms and control libraries can be used to maintain mappings, but technology alone does not create integration. Effective implementation depends on accountable ownership, reliable asset and data inventories, contractual visibility, cross-functional incident processes and evidence-based assurance.

10. PROPOSED MATURITY MODEL FOR FUTURE EMPIRICAL VALIDATION

Table 3 presents a future empirical extension of ICCPGF that can assess each domain using five maturity levels. These levels are proposed as research constructs and are not presented as validated performance thresholds.

Level	Descriptor	Indicative Characteristics
1	Fragmented	Siloed ownership; reactive compliance; incomplete inventories; limited supplier visibility.
2	Defined	Policies and responsibilities documented; periodic assessments; inconsistent integration.
3	Integrated	Common control mapping; linked cyber/privacy/vendor risk; coordinated incident escalation.
4	Measured	Risk-based metrics; continuous supplier monitoring; evidence-driven assurance; tested resilience.
5	Adaptive	Governance responds dynamically to threat, regulatory, architectural and business change; lessons learned systematically reshape controls.

11. RESEARCH PROPOSITIONS FOR SUBSEQUENT STUDIES

P1: Organizations with integrated cybersecurity and privacy governance will demonstrate clearer accountability for cloud risks than organizations using functionally separate governance processes.

P2: Integrated third-party governance will be associated with greater traceability between supplier risk assessments, contractual requirements and operational assurance.

P3: Cross-functional incident-response processes will reduce governance delays between technical detection and privacy/regulatory assessment.

P4: Organizations using a common control library with multi-framework mappings will report lower duplication of compliance activity than organizations maintaining framework-specific control silos.

P5: Higher ICCPGF maturity will be positively associated with stronger evidence quality, more consistent risk escalation and more systematic post-incident improvement.

12. LIMITATIONS AND FUTURE RESEARCH

This study has several limitations. First, ICCPGF is a conceptual framework and has not been empirically validated. Second, regulatory applicability varies by organization, sector, processing activity and jurisdiction; the comparative mapping should therefore not be interpreted as legal advice or as a declaration of compliance. Third, the historical cutoff of 30 June 2024 intentionally excludes later regulatory and standards developments. Fourth, high-level framework comparison cannot capture every sector-specific or contractual requirement.

Future research should validate ICCPGF through interviews with cybersecurity, privacy, legal, GRC and cloud professionals; surveys measuring governance maturity; and case studies involving regulated organizations and cloud service providers. The maturity model proposed in Section 10 offers one basis for such empirical assessment across the six domains. Additional research could also examine AI-enabled cloud services, cross-border data transfers, third-party concentration risk and the relationship between privacy engineering and cybersecurity operations.

13. CONCLUSION

Cloud computing makes cybersecurity, privacy, third-party and regulatory risks increasingly interdependent. NIST CSF 2.0, ISO/IEC 27001, Saudi cybersecurity controls and privacy regimes provide valuable but differently scoped governance mechanisms. The central challenge for regulated organizations is therefore not the absence of frameworks, but the fragmentation of accountability and implementation across them.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

The proposed Integrated Cloud Cybersecurity and Privacy Governance Framework (ICCPGF) addresses this challenge through six connected domains: governance and accountability; integrated risk assessment; data protection and privacy; cloud and third-party security; incident response and resilience; and assurance and continuous improvement. By mapping existing requirements into a common governance architecture, organizations can improve traceability, reduce duplicated compliance activity and strengthen coordination among security, privacy, legal, technology and risk functions. Empirical validation remains necessary before the model can be treated as a tested maturity or performance framework.

REFERENCES

1) Cloud Security Alliance. (2021). Cloud Controls Matrix v4. Cloud Security Alliance.
2) European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.
3) International Organization for Standardization. (2015). ISO/IEC 27017:2015 — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. ISO.
4) International Organization for Standardization. (2019). ISO/IEC 27018:2019 — Code of practice for protection of personally identifiable information in public clouds acting as PII processors. ISO.
5) International Organization for Standardization. (2019). ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. ISO.
6) International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.
7) International Organization for Standardization. (2022). ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks. ISO.
8) National Cybersecurity Authority. (2019). Critical Systems Cybersecurity Controls (CSCC-1:2019). Kingdom of Saudi Arabia.
9) National Cybersecurity Authority. (2020). Cloud Cybersecurity Controls (CCC-1:2020). Kingdom of Saudi Arabia.
10) National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing (SP 800-145). https://doi.org/10.6028/NIST.SP.800-145
11) National Institute of Standards and Technology. (2012). Cloud Computing Synopsis and Recommendations (SP 800-146). https://doi.org/10.6028/NIST.SP.800-146
12) National Institute of Standards and Technology. (2018a). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018
13) National Institute of Standards and Technology. (2018b). Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev. 2). https://doi.org/10.6028/NIST.SP.800-37r2
14) National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5
15) National Institute of Standards and Technology. (2022). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Rev. 1). https://doi.org/10.6028/NIST.SP.800-161r1
16) Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
17) Rigopoulos, K., Quinn, S., Pascoe, C., Marron, J., Mahn, A., & Topper, D. (2024). NIST Cybersecurity Framework 2.0: Resource & Overview Guide (NIST SP 1299). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1299
18) Saudi Data & AI Authority. (2023). Personal Data Protection Law and Implementing Regulations. Kingdom of Saudi Arabia.
19) UK Parliament. (2018). Data Protection Act 2018. United Kingdom.

Research Integrity and Historical-Cutoff Note

The manuscript uses 30 September 2024 as its historical evidence cutoff. The cutoff refers to the body of material analyzed; it does not represent or imply a publication date. Any journal submission should state the true submission, acceptance and publication dates. Before submission, all citations should be checked against the target journal's author instructions and the final manuscript should undergo a source-by-source reference audit. Later revisions of regulatory instruments should not be retrospectively attributed to the 2024 evidence base.

