International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

Data Governance Challenges in ITSM Platform Transitions

Mahesh Kumar Damarched

Enterprise Programmer Analyst, Louisville, Kentucky, USA

Email: mahesh.damarched@gmail.com

ABSTRACT: Migration of IT Service Management (ITSM) platforms changes the system that contains the history of operations and compliance evidence. This is not only a technical transfer but also the preservation of governance. When incidents, problems, changes, assets, and approvals are migrated to a new platform, data meaning drift, incomplete histories, broken relationships between records, and timing gaps that influence reporting and service level monitoring are the most frequent failures. Governance is the stabilizer since it establishes ownership, definitions, and rules of how records ought to be created, protected, retained, and validated prior to and after cutover. The paper explains the prominent data governance issues in the context of the transition of the ITSM platforms. It does so while focusing on data quality management, integrity protection, compliance with regulations, and auditability and traceability of actions between systems and teams. It also assesses the potential of implementing governance by way of migration planning, mapping standards, gradual implementation, organized validation processes, and constant monitoring, and it recognizes that the speed of change in the cloud era and the integration of tools increases the scope of governance. The discussion relates governance controls to ITSM practices like incident, change, event, and asset management, and how automation, analytics, and transparent stakeholder management can minimize operational impact and preserve evidence chains so that audits are possible.

KEYWORDS: Data Governance, ITSM Platform Migration, Data Integrity, Regulatory Compliance, Auditability and Traceability, Data Quality Management

I. INTRODUCTION

The ITSM platforms serve as the working memory of Information Technology (IT) in organizations. From the tickets, what was broken, who sanctioned such changes, which assets were involved, which customers were impacted, and whether there was service fulfillment can be captured by the ITSM platforms. Once that record is transferred to a new platform, the continuity becomes weak. Vadlamani et al. observe that cross-platform migration may 'miscarry' in the form of incompatible data formats and compatibility issues that may result in the end of transfer, and they also cite downtime as a frequent risk that must have strategies that minimize the impact[48]. Their focus on assessment, planning, execution, and validation phases even in data warehouse scenarios are easy to transfer to ITSM migrations, where validation is required to encompass not only row counts but also operational semantics[40],[48]. It may be deemed to incorporate a priority field that continues to lead to escalations as intended and whether timestamps retain the Service Level Agreement (SLA) calculations. This is more acute as records of ITSM are employed in the continuous decision-making process, as one corrupted audit field may cause a chain of evidence of a complete control test, as reflected by Ramakrishnan [35].

The issues of data governance when it comes to migrations between platforms are that it ensures the process of shifting the migration does not become an integrity risk. Lebaea et al. define data governance as a collection of frameworks that help direct the entire lifecycle of data, and align with the business requirements and compliance requirements, and they specifically reference the problem of data migration as being a frequent problem when upgrading a system[25]. Along with their review, the alignment of the governance with the business strategy and frequent updates of policies is consistently related to stable operations, and 78% of the reviewed studies report that their continuous monitoring, frequent updates, and data quality checks are linked to stable operations of IT[25]. Nookala and Villamil et al. supplements this perspective, claiming that digital transformation requires adaptive governance; this is also supported by Fajrillah et al[10],[32],[50]. This is since rigid forms of governance withstand high-velocity data settings, and the suggested transformation is the transition to reactive control towards ongoing monitoring that is capable of identifying compliance risks at an early stage.

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

The purpose of this research study is to explain the governance issues that are encountered when it comes to the process of migrating to ITSM platforms, and to trace the issues to controls capable of maintaining integrity, compliance, and auditability. The scope remains on disputable governance issues. These are areas that include data quality checks, access controls, audit log continuity, retention and deletion policies, encryption, and traceable change tracking. Under controlled conditions, Samala and Prayitno and Aprili explains that compliance frameworks like General Data Protection Regulation (GDPR), System and Organization Controls 2 (SOC 2), and Health Insurance Portability and Accountability Act (HIPAA) mandate high levels of security, privacy, and integrity, and believes that automation is more effective at mitigating human error and ensuring that compliance work stays the same, regardless of the organization[33],[41]. Cloud environments make the stakes even higher; according to Jyoti, cloud makes changes frequent and complex[21]. With efficient automation, the lead time of change can be as much as 70% shorter, rollbacks can be up to 40% fewer, and the amount of effort to prepare audits can be reduced by 60%[21]. Those outcomes give a viable justification to approach governance in the process of migration as a performance and risk issue, as opposed to a documentation activity.

II. DATA GOVERNANCE FUNDAMENTALS

Lebaea et al. establish data governance as a framework that assists in organizing the data collection, storage, processing, usage, and sharing, and ensuring that such an undertaking remains aligned with business goals, compliance with legal requirements, and ethical issues[25]. This definition proves useful in the context of ITSM migrations, as it puts the emphasis on governance as a type of operating system [15],[30]. This explanation makes data decisions, rather than being a policy enforcer, as stipulated by Gudepu and Eichler[13]. Practically, rules of governance manifest themselves as repeatable rules: which fields should be regarded as authoritative records about an incident, what fields must be obligatory, who is permitted to edit it, how long it must be retained, and how change histories are kept. Nookala builds on this argument by stating that conventional methods of governance are not always effective in high-velocity data ecosystems[32]. They describe adaptive governance as both flexible and responsive, with automation and real-time analytics enforcing policies that can adapt to emerging risks, such as privacy demands and mixed structured and unstructured data. Such a change is significant in ITSM since the platforms are now connected to Development and Operations (DevOps) tools, cloud policy engines, and security monitoring systems. Such a connection results in ITSM data flow being broader and quicker than the past siloed service desks.

Data governance is an evolving, cross functional management program which makes the roles and responsibilities of governance more obvious with a changing platform[44]. Lebaea et al and Momani propose governance committees and step-by-step processes in case of upgrades, and they emphasize the importance of aligning governance to business strategy to ensure governance facilitates system resilience rather than dragging down work[25],[31]. In ITSM migrations, the stakeholders are not merely the data owners and the IT leaders. They are also compliance officers, security teams, process owners, and operational teams that rely on proper records to make a response to incidents and change approvals. Jyoti cautions that change processes that rely on email and spreadsheet support have poor traceability and compliance gaps and suggests that there should be governance involvement in the enforcement of standardized workflows and integration of tools[21]. The stakeholder image becomes larger as vendors are considered, as they can affect data handling, security setup, and migration tools selections, thus impacting auditability and compliance posture[41].

The main elements of governance are policies, standards, and processes that can be implemented and verified. Lebaea et al. bind governance power to constant monitoring, frequent policy changes, and data quality verification, and such elements can be transformed into migration controls, such as data profiling prior to migration, field mapping criteria for field transformations, and post-migration validation checkpoints[25]. Nookala relates adaptive governance to automation and machine learning that may enforce policies in real time, which is pertinent when the migration of tickets is on a large scale or when new integrations create new data fields that require classification and protection[32]. According to Samala, audit trails are mandatory in organizations that deal with sensitive data, and the author notes that audit logs include information about who accessed or changed information and when, which makes audit logging a component of governance with quantifiable results[41]. As these policies and mechanisms are incorporated in the ITSM workflows, the governance is visible in the form of system behavior which involves measures where access control principles limit sensitive fields, encryption secures stored data, and audit records maintain the evidence trail[41].

The concept of data governance is pertinent to the setting of ITSM platforms directly in that the ITSM platform stores both operational and compliance evidence simultaneously[7]. Samala describes Jira as a tool that can automate workflow steps, notifications, assignments, and approvals, and they believe that this assists in maintaining compliance

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

uniformity in large distributed groups of workers[41]. That is important in the case of migration since the governance must be migrated along with the data. Machaladze explains that integrating Jira significantly decreases the number of unresolved incidences and enhances overall user experience[27]. A record of an incident can be migrated, but the new platform can lose the history of its original approval or change history; the organization may still be able to close its tickets, but it cannot demonstrate that it was being controlled in audits. Jyoti demonstrates that change velocity in the cloud era puts pressure on manual governance, and that is why governance should have the enforcement features, such as policy-as-code and orchestration integration[21]. Vadlamani et al. advocate elaborate mapping and transformation planning, which is consistent with the function of governance in making definitions of the fields, the way they need to be turned into, and the acceptable quality upon the move[48].

III. COMPLIANCE AND DATA INTEGRITY RISKS

Regulatory requirements influence the appearance of ITSM data and its protection, and it is not a mere hypothetical aspect of the high-risk environments. Samala characterizes GDPR, SOC 2, and HIPAA as systems that demand robust data security, data privacy, and data integrity controls[41]. They compare GDPR with its emphasis on the protection and rights of personal data, with the ruminations of SOC 2 with its trust service requirements, and HIPAA with its healthcare orientation. This is a consistency that is also adopted by Ilochonwu in addressing the operations of the agencies[17]. When dealing with huge amounts of sensitive information, compliance is challenging to ensure in the manual process, which they alternate with automation as a method to keep compliance activities the same and minimize the chances of omitted steps[41]. Compliance gaps are associated with manual change control techniques that are not integrated, lack traceability, and are liable to audit failure, and with observation being carried down into migrations where the data can be transformed, access rules may change, and evidence trails may be fragmented[21]. Salloum recommends offering rules for data management and ensuring constant monitoring to maintain regulatory compliance[39].

The risk in data quality increases exponentially during platform transitions[42]. This is because during the process, the movement of the data exposes inconsistencies in the data that were covered by the previous system. Vadlamani et al. project that incompatible formats and compatibility problems may result in errors in transfer and endanger integrity[48]. They proceed to note that downtimes can be disruptive unless migration is scheduled to minimize interference. In ITSM, data quality issues are manifested by a duplicate record, missing fields, inconsistent categorization, or broken relationships between records, such as loss of an incident with a connected change request. Lebaea et al. characterize data migration problems as a frequent problem in upgrades, and the evaluation of them links data governance to the enhancement of data quality and operational effectiveness, which means that the governance controls need to be operational during the process of migration planning and implementation[25]. Nookala states that adaptive governance incorporates real-time analytics and automation to implement the policy that may be used to carry out constant quality checks in the case of data flowing in bulk[32].

Integrity risks do not occur in terms of wrong data. Within a regulated environment, integrity involves the demonstration of the fact that records were not changed unlawfully. To ensure data integrity Kudaibergenova recommends a unified data model, which defines standard fields, relationships, and chain of command that apply across systems[23]. According to Samala, audit logs include information about who accessed or modified data and when, and they position such logs as the key to adherence to GDPR, SOC 2, and HIPAA[41]. Samala also states that the actions should be traced until creating and deleting tickets, and modifying them, user information, and timestamps to facilitate the accountability and data integrity needs[41]. It is stated in the article by Jyoti that cloud environments introduce the risk of configuration drift, obscure dependencies, and uneven policy enforcement that may result in security mal-configurations and policy violations[21]. Lakdinu argue that AI-driven environment requires robust security structures[24]. In the case where an ITSM migration is accompanied by a change in cloud tooling, the risk to integrity increases. A record could be correct, but the control environment below might no longer maintain the requirements of who is allowed to update that record and/or how that review is performed.

The mitigation measures in the given literature are based on planning, automation, access control, encryption, and constant monitoring. Vadlamani et al. focus on having a structured plan with elaborate mapping and transformation plans and stimulate the use of automated migration tools to minimize manual errors[48]. Samala discusses the ability of Jira to create comprehensive reports out of the audit logs information[41]. This creation allows the internal auditing and compliance assessment to be filtered by action, user, or period in time, thus discouraging a lack of strong accountability in migration[26]. She goes further to state that encryption of transit and rest assists the security needs of SOC 2 and HIPAA, whereby transport layer security helps to protect data in transit, and at-rest encryption helps to safeguard data

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

that is stored, even in cases where storage is accessed[41]. It is essential to connect the stable operations with regular policy updates, monitoring, and data quality checks, and adopt robust implementation strategies in stages in case of upgrades, which might help alleviate the migration shock, and governance mechanisms that can evolve over the years. The evidence of performance presented by Jyoti, which has led to the reduction of lead time and rollback incidents and better preparation of audits, justifies the adoption of automated pipelines and policy enforcement as a mitigation strategy in the migration era rather than a metric that is nice to have after the migration[21].

IV. GOVERNANCE FRAMEWORKS DURING MIGRATION

A migration strategy that uses ITSM data as a stack of export files is pointless because ITSM is a control surface. The literature available in ITIL, in IT governance research, and in data governance is all based on the same practical concept, as garnered from Kauko[22]. They follow the design that governance should be part of the value stream, not tied on at the end. According to Dhanabal and Dande, ITIL 4 is less about strict process compliance and is more of a 'service value system' that favors governance, improvement, and service delivery in unstable worlds of technology[6],[8]. It also ensures that the framing is appropriate to migration work since the migration itself is a value stream with its own inputs, controls, and quantifiable outputs. In the case of cloud conditions, Dhanabal compares centralized governance and manual documentation with distributed control and Application Programming Interface (API) automation and claims that a successful cloud service management predominates automation as the main process and considers manual steps as an exception[8].

The latter relates to adaptive data governance as that aspect is linked to that point. Research holds that in dynamically changing ecosystems, governance should be flexible and responsive and that responsiveness will frequently rely on automation and constant monitoring, rather than periodic review cycles. The ITSM governance dilemma lies in the conflict between standardization and flexibility, as projected from Tolok et al. standardization context[47]. There are reports of agile methods being more adaptive and ITIL having more structured management in tandem with business requirements, and the literature evidence that the practical risk of too much rigidity is a slow response and too much flexibility stands to compromise the integrity of control[28]. When migration governance pays no attention to that balance, it is likely to result in a brittle implementation of compliance by paperwork. It may also cause a rapid transition that becomes traceable and audit-ready.

The initial governance checkpoints are data mapping and migration planning, since this is where the meaning may be quietly lost. Vadlamani et al. list typical barriers to migration, like format differences, compatibility issues, and downtimes, and emphasize organized planning and validation[48]. With ITSM migrations, field-to-field matching will be insufficient; mapping will need to preserve relationships and evidence paths, including incident-to-problem links, change approvals, timestamps used in calculating SLA, and historical assignment changes, among other options that foster accountability. According to Boppana data governance secures data by implementing robust measures to protect data from breaches or unauthorized access[4]. Governance literature supports the idea that upgrade failures are mainly because of the data migration difficulties, and thus, the use of phased approaches and governance committees to deal with risks throughout change adoption is advised. Agile ITSM research contributes to the helpful operational layer. In the support-engineer interview focus areas, Mandi encompasses data logs in troubleshooting and the purpose of collaboration tooling, which can be converted into a practical mapping requirement when migrating the data[28]. Generally, logs, attachments, and ticket histories should not be summarized and truncated during mapping, this is since both troubleshooting and audit evidence will suffer.

The control mechanisms should be enforced, observable, and testable as long as the migration is ongoing. Samala gives an explanation in the Jira compliance automation framework where the audit logs document the person who viewed or manipulated data and the time, and they place this at the heart of accountability in GDPR, SOC 2, and HIPAA[41]. Samala also outlines encryption on transit and rest as a security expectation, and TLS is utilized in transmitting data and encryption in rest safeguard the data in storage even when the storage is visited[41]. The latter are governance controls in the most straightforward sense. They limit what can be done and generate testable evidence. Compliance monitoring of machine learning is taken to nearly real-time monitoring. The machine learning (ML) model that processed service logs, incident records, and change management data decreased the time of detection of compliance issues by 70%, the accuracy rate increased by 75% to 92%, and the use of resources decreased by 50%[19]. In addition, it revealed the unresolved concerns in terms of data privacy, transparency, and integration issues. Such results are important to migration governance as migrations are frequently operated with mixed states (simultaneously old and new platforms), and automated surveillance can minimize the time gap between an issue being presented and an issue being observed. This defined the adoption of ITSM framework by Adiningtyas et al [1].

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

The stakeholder control and responsibility broaden in cloud-based migrations since the vendor can be included in the management controls. The existing research on vendor risk management emphasizes the fact that Vendor Risk Management (VRM) is not about paperwork in procurement but a governance discipline that relates dependencies on third parties to their risk on the enterprise. Faruq describes the governance of vendor risk using the principal-agent theory and the risk governance theory, stating that the cloud vendors possess information advantages, which result in monitoring gaps, and that the organizations should close such gaps by using audits, incentives, and governance mechanisms as part of enterprise risk management[11]. The argument can be useful in ITSM migration planning since the platform vendors, implementation partners, and even cloud providers can influence the security configuration directly, the logging options, retention options, and even the completeness of the migrated histories. Weak oversight has its consequences, which are outlined in the same review by research that asserts that third-party providers contributed to an increasing proportion of breaches and that incidents involving vendors are capable of producing a ripple effect of reputational and financial harm[11]. That, in a migration context, does not imply that vendor alignment should be at the mercy of generic SLAs. Governance ought to demand detailed audit rights, control test evidence requirements, and the clarity of responsibility boundaries regarding incident response and data protection, as projected.

Examples of cases from the literature studies indicate the appearance of good governance when it is not described, but when it is practiced. Dhanabal and Gangula, defines ITIL v4 practices, including collaborative investigation, mapping dependencies between services, and tracking the version of infrastructure-as-code and automated response playbooks, and relates them to the measurable improvements, including faster Mean Time to Recovery (MTTR) and higher first-time root cause identification in the cloud environment[8],[12]. Here, governance is expressed through repeatable and structured behavior: alerts are turned into tickets, ownership is assigned with rapidity, deployments are connected with incidents, and changes are tracked as code versions[8]. The cultural layer introduced by agile ITSM evidence is what commonly determines the success or failure of these controls to take hold. Support engineers have explained the importance of immediate communication tools, knowledge sharing platforms, and constant learning cultures that minimize unnecessary problem-solving and fast resolution of problems[28]. When these practices are carried into migration governance, they strengthen the migration's ability to preserve operational continuity and evidence integrity at the same time. This is since governance is sustained by real team routines, not a one-time checklist.

V. AUDITABILITY AND TRACEABILITY

Auditability refers to the fact that some evidence can be provided indicating what was done to the data and why choices have been made. This is uncompromising in the migration process of ITSM since audit trails are frequently legally and regulatory binding. Auditing also aid in accountability and transparency within the company and the auditors[5]. Samala contextualizes audit trails as essential in organizations that work with sensitive data since audit logs record user activities, in addition to timestamps and ticket manipulations, and she associates that with accountability and integrity in GDPR, SOC 2, and HIPAA[41]. Auditability takes two sides once the migration is started. One of them is operational: teams require traceability to investigate and recover service promptly in case of incident spikes during a changeover. The other one is compliance: the organization will still need to demonstrate that change approvals, access controls, and incident handling were done as needed, even as systems are changing. Dhanabal emphasizes that ITIL v4 prioritization and grouping are business impact and value streams-driven instead of template-based, and they write that active stakeholder communication and alignment with development pipelines are beneficial in keeping track of response and context in the event of a disruption[8]. The same integration provides the creation of a traceable connection between changes and incidents. This is essential in post-incident review and defense of the audit.

The traceability tools and methods in the current ITSM transitions are strongly based on automation and integration. Dhanabal defines infrastructure-as-code version tracking as a method to keep full records of modifications, replace a guess-based approach to troubleshooting with a code-based one[8]. They also refer to automated response playbooks that translate organizational knowledge into operational processes. These processes are important when migrating as the code repositories and Continuous Integration / Continuous Delivery (CI/CD) pipelines become the source of truth of the changes, and traceability must follow these changes. The support engineers of agile ITSM environments focused on collaboration platforms and automation tools, and there was an explicit focus area of the interview on the evaluation of the data logs in troubleshooting[28].

That practice is a traceability requirement: where logs, incident timelines, and associated deployment data are not maintained through the migration process, both troubleshooting and audit reconstruction become increasingly sluggish and less dependable in compliance monitoring, Jain demonstrates that ML models are able to process service logs, incident records, and change data and identify anomalies indicating compliance problems more quickly and with

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

greater accuracy than a human monitoring the data[19]. Such monitoring facilitates traceability through raising patterns of anomaly, which can alert to a policy deviation in the process of migration, as reflected by Jain[19]. The necessity of data privacy safeguards and model transparency, which links traceability to explainability and accountability.

When auditability is aimed at, reporting and monitoring structures are helpful when they are based on the production of repeatable evidence. According to Samala, continuous monitoring in Jira is achieved by audit log review, compliance dashboards, real-time metrics, and internal audit checks that will ensure that automated workflows are applying policies as planned[41]. Findings also mentions that another technology is Artificial Intelligence (AI) and machine learning (ML) to monitor predictive compliance and blockchain to have audit trails that are not tampered with[41]. These concepts align with real-life reporting requirements of ITSM migration, including demonstrating that access to sensitive tickets continued to remain within legitimate roles, that changes that posed high risk were approved, that incident communications were done with a regular rhythm, and that historical data was not lost in the new platform.

The auditability is linked to speed in the research of cloud governance. According to Dhanabal, the focus of cloud environments is on API automation and continuous integration, and thus traceability frequently resides in the system logs, pipelines, and in the version control records as opposed to written documentation[8]. Guidance on data governance identifies stability with ongoing monitoring and frequent updates, data quality checks preventing slow drift turning into an audit failure[25], and adaptive governance work asserts the need to have a real-time oversight that can keep up with the changing environment[32]. Another requirement is vendor risk governance. Here, Faruq cautions that there are gaps in monitoring since vendors are in a better position to know their security position and operational habits, auditability is therefore immune to contractual and governance arrangements that ensure that evidence is acquired on time[11].

VI. CASE STUDY

Puupponen demonstrates that in companies, the development of ITSM processes is often initiated by the need to document the current status, label the pain points, and design a target process that can comply with the local constraints, and the order process-first turns into a migration guardrail since it helps to define what the data should make possible prior to any transfer[34]. The cloud-based Software as a Service (SaaS) environment defines event management design as an orderly endeavor in which monitoring and alert monitoring are synchronized to the service rhythm, which is significant as event streams usually supply incident generation and escalation routes in ITSM. A parallel run is more controlled by transition discipline, Huhtala associates better transition services with more specific handovers and steps, and the same mechanics minimize ambiguity when the work is divided between an old and new platform[16].

The migration environment is a cloud-affected organization in which incident responses, change approvals, asset reports, and audit reporting are based on the ITSM system of record. Jassal associates the contemporary ITSM development with automation, analytics, and integration requirements and cautions that governance should inhibit tool fragmentation, and tension is the reason why migrations tend to be coupled with technical change and governance redesign[20]. Inavolu explains transformation barriers, including cultural resistance, process misalignment, and tool complexity, and the barriers enable one to understand why migration work evolves into adoption work[18]. Governance benefits associated with a more defined structure of service management in a pilot of the public sector are described by Sarwar et al.[43], and audit expectations support the necessity of risk and control traceability, which Miharja and Ginardi and Vaya-Arboledas et al. link to internal audit effectiveness and use of Control Objectives for Information and Related Technologies (COBIT) 2019 and International Organization for Standardization (ISO) 31000:2018[29],[49]. Bharathan and Ramakrishnan et al. stipulate that COBIT is essential in controlling objectives and metrics of all the domains[3],[36].

The appearance of data quality and meaning drift was already observed in extraction and mapping. Vadlamani et al. risk transfer error during mapping, which is shallow because of the mismatch of formats and compatibility problems in the system when the mapping is shallow[48]. In this incident research observes that ambiguity and lack of uniformity in the definitions and practices can make standardization more difficult, and after migration, inconsistent reporting can occur. Asset data creates an additional burden; Harjanto and Aji state that ITIL 4-congruent asset management is based on a regular lifecycle record, but migrations usually reveal duplicates, a lack of ownership information, and missing links to incidents[14]. The effect of compliance risk compounded the move since auditability has to endure the transition. Audit logs are treated as part of accountability in regulated settings, and the lack of cloud-governance alignment and dependence on vendors introduces oversight risk[9],[11],[38],[41].

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

As a layer of governance and not a feature switch, controls were used. Lebaea et al. connect the stable operations to incessant overseeing, updates on policies, and data quality, and Nookala states that adaptive governance is based on automation and real-time monitoring that controls graded validation gates in parallel operations[25],[32]. The integrity controls were based on organized risk mitigation concepts and quality harmonization concepts made with the help of AI-integrated concepts of master data management [45],[46]. Blind spots were minimized by using ML-based guidance in detection. There is automation of workflows, which enhances consistency and traceability, as listed by Ravichandran et al.[37]. Migration continuity was considered a migration control. The ITSM digital commons work posits shared artifacts as a means of closing practice gaps and maintaining capability amid change and data strategy guidance cautions that migration may thwart AI and analytics value by allowing integration and quality failures [2].

VII. CONCLUSION

The report demonstrates that the issues in ITSM migrations have a predictable and interrelated nature in terms of data governance. The first signs of data quality problems, such as duplication, omission of a field, inconsistency in categorization, and broken links between records, among other are usually visible and readily apparent. Despite this, the latent risk is in the integrity and continuity of evidence, as approvals, timestamps, and change histories are the foundations of accountability. A transition remains justifiable when governance is seen as a functioning control system that proceeds to the post-migration process by extraction, with each domain of data having an explicit owner, and there being a shared understanding of how to map and transform. Validation should also test operational meaning, such as whether the escalations and SLA logic still work. It should also test audit readiness, such as whether the logs and histories left after the move are complete and traceable. Compensation areas of expectations take it a notch higher by laying down expectations of safe management of sensitive information, regular access controls, and being able to guarantee retention and deletion behavior. Cloud adoption and vendor reliance become more complex due to the speed of changes, the expansiveness of integrations, and the blurred responsibility lines of third parties, and thus, continued monitoring and clarified accountability are required post-go-live. Combined with automation and shared knowledge practices, governance can become integrated into workflows.

REFERENCES

1. Adiningtyas, G., Raharjo, T., Trisnawaty, N. W., & Yuniarti, R. (2024). Implementing project management integrated with ITIL: Case study in a fast-moving consumer goods company. *The Indonesian Journal of Computer Science*, *13*(4). https://doi.org/10.33022/ijcs.v13i4.4131
2. Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. *Applied Sciences*, *13*(12), 7082. https://doi.org/10.3390/app13127082
3. Bharathan, R. (2025). Mastering technology audit quality assurance: A framework for auditors. https://www.tdcommons.org/dpubs_series/8120/
4. Boppana, V. R. (2021). Ethical considerations in managing PHI data governance during cloud migration. Educational *Research (IJMCER)*, *3*(1), 191-203. https://www.ijmcer.com/wp-content/uploads/2024/10/IJMCER_Z0310191203.pdf
5. Carter, D., Thompson, E., Nguyen, C., Robinson, A., & Paul, C. (2024). Monitoring and logging frameworks for migration troubleshooting and auditing. https://www.researchgate.net/profile/Charles-Paul-8/publication/394458299_Monitoring_and_Logging_Frameworks_for_Migration_Troubleshooting_and_Auditing/links/689c0bbcdaa95834904ed11b/Monitoring-and-Logging-Frameworks-for-Migration-Troubleshooting-and-Auditing.pdf
6. Dande, F., Li, X., Shofoluwe, M., & McLeod, A. (2024, October). Artificial Intelligence integration in IT Service Management: An ITIL configuration management process review. In Proceedings *of the International Conference on Industrial Engineering and Operations Management, Detroit, MI, USA* (pp. 9-11). https://www.academia.edu/download/119271703/Artificial_Intelligence_integration_in_IT_Service_Management_An_ITIL_configuration_management_process_review.pdf
7. de Souza, L. K., & Engstler, M. (2025). Sustainable transformation of IT service management: A review of the ITIL-framework and its alignment with circular economy principles. https://www.sdconference.org/uploads/1/1/4/7/11479227/15bc41566579198319ac.pdf
8. Dhanabal, P. (2025). Demystifying ITIL-based incident management in cloud environments. *Journal of Computer Science and Technology Studies*, *7*(8), 892-903. https://doi.org/10.32996/jcsts.2025.7.8.104
9. Efe, A. (2025). Risk modeling of challenges and opportunities in harmonizing traditional IT governance with emerging cloud governance frameworks. *Pamukkale Üniversitesi İşletme Araştırmaları Dergisi*, *12*(2), 411-435. https://doi.org/10.47097/piar.1741326

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

10. Fajrillah, A. A. N., Lubis, M., & Pasa, A. R. (2022). Towards the smart industry for the sustainability through open innovation based on ITSM (Information Technology Service Management). *International Journal of Advanced Computer Science and Applications*, *13*(6), 140-152. https://www.academia.edu/download/95300207/Paper_19-Towards_the_Smart_Industry_for_the_Sustainability_through_Open_Innovation.pdf
11. Faruq, M. O. (2024). Vendor risk management in cloud-centric architectures: A systematic review of soc 2, Fedramp, and ISO 27001 practices. *International Journal of Business and Economics Insights*, *4*(1), 01-32. https://doi.org/10.63125/j64vb122
12. Gangula, S. A (2025). A comprehensive review of ITIL frameworks for managing large-scale retail cloud operations and challenges. https://www.academia.edu/download/125423948/A_Comprehensive_Review_of_ITIL_Frameworks_for_Managing_Large_Scale_Retail_Cloud_Operations_and_Challenges.pdf
13. Gudepu, B. K., & Eichler, R. (2024). The role of AI in enhancing data governance strategies. *International Journal of Acta Informatica*, *3*(1), 169-186. https://www.yuktabpublisher.com/index.php/IJAI/article/view/196
14. Harjanto, A., & Aji, R. F. (2024). Improving IT assets management with ITIL 4 framework. *Jurnal Ilmu Komputer dan Informasi*, *17*(2), 127-143. https://doi.org/10.21609/jiki.v17i2.1195
15. Hasan, M. M., & Islam, M. M. (2023). Reinforcement learning approaches to optimize IT service management under data security constraints. *American Journal of Scholarly Research and Innovation*, *2*(02), 373-414. https://doi.org/10.63125/z7q4cy92
16. Huhtala, J. A. K. (2021). Improvement of transition data centre services process. https://urn.fi/URN:NBN:fi:amk-2021090117366
17. Ilochonwu, I. A. (2024). Information technology governance in cloud computing a framework of risk management and compliance. *IJIRT 170269 International Journal of Innovative Research In Technology*. https://www.academia.edu/download/120546854/Information_Technology_Governance_in_Cloud_Computing_A_Framework_of_Risk_Management_and_Compliance.pdf
18. Inavolu, M. (2025). Challenges in ITSM digital transformation: A case study. https://urn.fi/URN:NBN:fi-fe2025060963061
19. Jain, A. (2025). Automating compliance monitoring in ITSM platforms using machine learning. *Scientific Journal of Artificial Intelligence and Blockchain Technologies*, *2*(4), 16-18. https://doi.org/10.63345/sjaibt.v2.i4.303
20. Jassal, H. (2025). The evolution of IT service management: Navigating digital transformation in the modern enterprise. *Journal Of Engineering And Computer Sciences*, *4*(8), 327-339. https://sarcouncil.com/2025/08/the-evolution-of-it-service-management-navigating-digital-transformation-in-the-modern-enterprise
21. Jyoti, S. N. (2025). ITSM based change management automation in cloud environments: A cross sector empirical study. *Review of Applied Science and Technology*, *4*(02), 440-472. https://doi.org/10.63125/xvjst226
22. Kauko, J. (2021). Development of event management process (ITSM) for a cloud-based SaaS company. https://www.theseus.fi/bitstream/handle/10024/510368/Kauko_Jonas.pdf?sequence=2
23. Kudaibergenova, A. (2020). Unified reporting on patch status and ticket resolution times. https://www.researchgate.net/profile/Selva-Kumar-49/publication/394013748_UNIFIED_REPORTING_ON_PATCH_STATUS_AND_TICKET_RESOLUTION_TIMES/links/6883d39800a2407910a414ed/UNIFIED-REPORTING-ON-PATCH-STATUS-AND-TICKET-RESOLUTION-TIMES.pdf
24. Lakdinu, P., P., K. (2025). Data governance's role in digital transformation a systematic literature review. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1967803&dswid=5811
25. Lebaea, R., Roshe, Y., Ntontela, S., & Thango, B. A. (2024). The role of data governance in ensuring system success and long-term IT performance: A systematic review. https://www.preprints.org/frontend/manuscript/3beb8211cdc66768e0595dbf1d9c4f83/download_pub
26. Leon, P. (2020). Creating accountability and increasing efficiency by implementing an IT service management solution. https://scholarworks.lib.csusb.edu/etd/1047/
27. Machaladze, O. (2025). IT infrastructure management in educational institutions using ITIL framework and Atlassian products. *American Journal of Engineering Research*. https://www.researchgate.net/profile/Otari-Machaladze/publication/392123403_IT_Infrastructure_Management_in_Educational_Institutions_Using_ITIL_Framework_and_Atlassian_Products/links/683588358a76251f22e94186/IT-Infrastructure-Management-in-Educational-Institutions-Using-ITIL-Framework-and-Atlassian-Products.pdf
28. Mándi, Á. (2024). *Agile IT service management: an analysis and enhancement of ITIL practices in corporate environments* (Doctoral dissertation). https://repositorio.ucp.pt/server/api/core/bitstreams/e185c455-22ed-4f00-9fce-9cedb53a937a/content

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

29. Miharja, I. S., & Ginardi, R. V. H. (2025). Evaluation of the effectiveness of audit management system (AMS) Using COBIT 2019 and ISO 31000: 2018 in the internal audit function. *Sebatik*, *29*(2), 343-360. https://doi.org/10.46984/sebatik.v29i2.2627
30. Mishra, A. (2019). Exploring ITIL and ITSM change management in highly regulated industries: A review of best practices and challenges. https://www.academia.edu/download/124599203/Exploring_ITIL_and_ITSM_Change_Management_in_Highly_Regulated_Industries_A_Review_of_Best_Practices_and_Challenges.pdf
31. Momani, D. A. M. (2024). The role of IT governance in organizations: Best practices for enhancing audit, control, and success. *Available at SSRN 5053120*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5053120
32. Nookala, G. (2024). Adaptive data governance frameworks for data-driven digital transformations. *Journal of Computational Innovation*, *4*(1). https://researchworkx.com/index.php/jci/article/view/16
33. Prayitno, G., & Aprili, R. (2026). Examining the role of information technology governance in enhancing risk management performance and Regula-tory compliance in multinational digital enterprises. *Integrated System and Management Technology*, *1*(1), 11-20. https://journal.apjikom.or.id/index.php/ISMaT/article/view/7
34. Puupponen, A. (2023). Developing the ITSM process of a case company. https://www.theseus.fi/bitstream/handle/10024/789738/Puupponen_Aleksi.pdf?sequence=2
35. Ramakrishnan, M. (2022). *Development and evaluation of it service management digital* commons-*a case study* (Doctoral dissertation, University of Southern Queensland). https://doi.org/10.26192/wq850
36. Ramakrishnan, M., Gregor, S., Shrestha, A., & Soar, J. (2025). Addressing knowledge gaps in ITSM practice with "learning digital commons": A case study. *Information Systems Frontiers*, *27*(3), 965-989. https://doi.org/10.1007/s10796-024-10483-0
37. Ravichandran, N., Inaganti, A. C., Muppalaneni, R., & Nersu, S. R. K. (2020). AI-Powered workflow optimization in IT service management: Enhancing efficiency and security. *Artificial Intelligence and Machine Learning Review*, *1*(3), 10-26. https://doi.org/10.69987/
38. Remella, S. (2025). Vendor alignment and governance models for large-scale cloud infrastructure initiatives. *International Journal of Emerging Trends in Computer Science and Information Technology*, 69-76. https://doi.org/10.63282/3050-9246/ICRTCSIT-109
39. Salloum, M., Toh, B., & Yare, T. Secure cloud migration challenges. https://www.researchgate.net/profile/Mohammad_Salloum3/publication/382968846_Secure_Cloud_Migration_Challenges/links/66b537df51aa0775f274fd20/Secure-Cloud-Migration-Challenges.pdf
40. Salo, V. (2020). IT service management system implementation. https://trepo.tuni.fi/bitstream/handle/10024/122178/SaloVesa.pdf
41. Samala, S. (2025). Automating ITSM compliance (GDPR/SOC 2/HIPAA) in Jira workflows: A framework for high-risk industries. *International journal of data science and machine learning*, *5*(01), 98-126. https://inlibrary.uz/index.php/ijdsml/article/view/108417
42. Sarmah, Simanta Shekhar. "Data migration." *Science and Technology* 8.1 (2018): 1-10. https://www.researchgate.net/profile/S-Sarmah/publication/336084389_Data_Migration/links/5d8d8bc892851c33e94074c8/Data-Migration.pdf
43. Sarwar, M. I., Abbas, Q., Alyas, T., Alzahrani, A., Alghamdi, T., & Alsaawy, Y. (2023). Digital transformation of public sector governance with IT service management–A pilot study. *IEEE Access*, *11*, 6490-6512. https://ieeexplore.ieee.org/abstract/document/10018341/
44. Shaffi, S. M. (2022). Enterprise content management and data governance policies and procedures manual. *International Journal of Science and Research (IJSR)*, *11*(8), 1570-1576. https://www.scholarprofiles.me/scholars/shamnadmohamedshaffi/publications/Enterprise%20Content%20Management%20and%20Data%20Governance%20Policies%20and%20Procedures%20Manual.pdf
45. Tadi, V. (2020). Optimizing data governance: Enhancing quality through AI-integrated master data management across industries. *North American Journal of Engineering Research*, *1*(3). https://najer.org/najer/article/view/7
46. Toapanta, S. M. T., Durango, R. H. D. P., Gallegos, L. E. M., Díaz, E. Z. G., Quintana, Y. J. M., Jimenez, J. N. M., ... & Trejo, J. A. O. (2022). Prototype to mitigate the risks, vulnerabilities and threats of information to ensure data integrity. *Adv. Sci. Technol. Eng. Syst. J*, *7*(6), 139-150. https://www.academia.edu/download/114676245/_.pdf
47. Tolok, G., Kozhemiakin, O., Didovets, V., Tkachenko, O., Chechyk, S., Vostrikov, S., ... & Borodavko, M. (2025). Standardization and certification of software in the field of information and communication technologies. *European Science*, (sge42-04), 145-171. https://desymp.promonograph.org/index.php/sge/article/download/sge42-04-048/3100
48. Vadlamani, S., Agarwal, N., Chintha, V. R., Shrivastav, E. A., Jain, S., & Goel, O. (2023). Cross platform data migration strategies for enterprise data warehouses. *International Research Journal of* Modernization *in Engineering, Technology and Science 5 (11): 1-10. https://doi. org/10.56726/IRJMETS46858*. https://www.academia.edu/download/118865420/fin_irjmets1727782658.pdf

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed, a Bimonthly Journal|

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806033

49. Vaya-Arboledas, Á., Ferrer-Oliva, M., & Medina-Merodio, J. A. (2025). Evolution and perspectives in IT governance: A systematic literature review. *Computers*, *14*(12), 520. https://doi.org/10.3390/computers14120520
50. Villamil, R. M., Restrepo-Carmona, J. A., Escobar, A., Aponte-Moreno, A., Herrera, J. A., Gutiérrez-Betancur, S. A., & Fletscher, L. (2025). An enterprise architecture-driven service integration model for enhancing fiscal oversight in supreme audit institutions. *Applied System Innovation*, *9*(1), 16. https://doi.org/10.3390/asi9010016