

Статья поступила в редакцию: 20.08.2026

Статья принята к публикации: 13.09.2026

Статья опубликована: 28.09.2026

УДК 004.9+338.2+658.5

Cloud-native EDI migration in retail: an organizational and managerial toolkit based on stage-gate governance and qualitative risk classification

Nikolaev Konstantin

Director of Software Engineering AiDiKom

USA, Carlsbad

E-mail: t6192148993@gmail.com

Миграция retail-систем EDI в cloud-native архитектуру: организационно-управленческий инструментарий на основе stage-gate и качественной классификации рисков

Николаев Константин

директор

по разработке программного обеспечения AiDiKom

США, Карлсбад

Abstract

Electronic Data Interchange (EDI) remains the primary method by which retailers exchange orders, invoices and shipment notices with trading partners, yet many retailers still operate these systems on on-premises infrastructure that constrains scalability as e-commerce volumes grow. The objective of this study is to develop an organizational and managerial toolkit for migrating retail EDI systems to a cloud-native architecture. Two research tasks are addressed: (1) to justify the governance stages of the migration process, and (2) to classify the technical risks associated with the transition to cloud-native EDI. Methodologically, the study applies the Stage-Gate project management approach to derive and justify governance stages and formal decision checkpoints, and a qualitative risk analysis method to identify and classify integration barriers and migration risks. The results are presented as two original analytical instruments: a five-pillar stage-gated governance model specifying activities, decision gates and accountability for each stage of EDI migration (Table 1), and a risk classification matrix linking technical migration risks to their business implications for the retailer and to mitigation methods derived from the proposed model (Table 2). Published industry evidence is used in the discussion to assess the practical applicability of the toolkit. The proposed toolkit gives retailers a structured and auditable basis for planning EDI migration and for allocating managerial responsibility across its stages.

Библиографическое описание: Николаев К. Миграция retail-систем EDI в cloud-native архитектуру: организационно-управленческий инструментарий на основе stage-gate и качественной классификации рисков // Universum: технические науки : электрон. научн. журн. 2026. 9(150). URL: <https://7universum.com/ru/tech/archive/item/23397>

For citation: Nikolaev K. Cloud-native EDI migration in retail: an organizational and managerial toolkit based on stage-gate governance and qualitative risk classification // Universum: Technical Sciences : electronic scientific journal. 2026. No. 9(150). Available at: <https://7universum.com/ru/tech/archive/item/23397>

Аннотация

Электронный обмен данными (EDI) остаётся основным способом передачи заказов, счетов-фактур и уведомлений об отгрузке между ритейлерами и их торговыми партнёрами, однако многие компании по-прежнему эксплуатируют такие системы на локальной инфраструктуре, что ограничивает масштабируемость при росте объёмов электронной коммерции. Цель исследования — разработать организационно-управленческий инструментарий миграции retail-систем EDI в cloud-native архитектуру. Решаются две исследовательские задачи: (1) обосновать управленческие стадии процесса миграции и (2) классифицировать технические риски перехода к cloud-native EDI. Методологически исследование опирается на подход проектного управления Stage-Gate, используемый для обоснования стадий управления и формальных точек принятия решений, а также на метод качественного анализа рисков для выявления и классификации интеграционных барьеров и рисков миграции. Результаты представлены двумя оригинальными аналитическими инструментами: пятикомпонентной stage-gate моделью управления, определяющей мероприятия, точки контроля и распределение ответственности на каждой стадии миграции EDI (Таблица 1), и матрицей классификации рисков, связывающей технические риски миграции с их бизнес-последствиями для ритейлера и методами их снижения в рамках предложенной модели (Таблица 2). Опубликованные отраслевые данные используются в разделе обсуждения для оценки практической применимости инструментария. Предложенный инструментарий даёт ритейлерам структурированную и проверяемую основу для планирования миграции EDI и распределения управленческой ответственности по её стадиям.

Keywords: Cloud EDI, electronic data interchange, retail integration, e-commerce, migration, Stage-Gate governance, qualitative risk analysis, risk classification.

Ключевые слова: Cloud EDI, электронный обмен данными, интеграция в розничной торговле, электронная коммерция, миграция, Stage-Gate управление, качественный анализ рисков, классификация рисков.

Introduction

Retailers have used Electronic Data Interchange (EDI) for a long time to pass orders, invoices, and shipment details between suppliers and customers [1]. For years, the usual way was to keep the systems on servers inside company offices. Those setups managed normal daily volumes without too much trouble. But when online shopping picked up speed, the old systems started showing their age. Hardware upgrades turned expensive, maintenance windows forced service stops, and bringing in a new partner from another country often meant weeks of manual work and testing.

This pattern has been observed across multiple retail companies in IT governance contexts. Online sales keep growing every year, and retailers now need to handle large transaction numbers without any delays. Traditional on-premises systems cannot scale easily or stay up all the time [2].

Cloud-native EDI gives a better practical answer. It runs on cloud services and is made from small independent pieces — microservices and containers — that grow or shrink as demand changes [3]. The system does not need a full stop for updates or repairs. This paper explains the practical benefits for retailers, outlines a structured migration approach, and demonstrates how the transition improves customer service outcomes.

A governance framework has been developed based on IT governance practices and vendor negotiation experience. It has five pillars and clear approval points at every stage. The framework keeps risks under control and turns the migration into an ordinary business step rather than a risky adventure [5].

The paper stays exactly on the approved topic. It covers the move to cloud-based EDI that removes legacy infrastructure barriers, so retailers can process millions of transactions daily with zero downtime and full scalability for global marketplaces. It draws on industry practices to establish best practices for migrating on-premises systems to cloud EDI while making sure data flows stay secure and new trading partners join quickly. Finally, it shows how automation of invoice reconciliation and shipment tracking turns EDI into a real competitive edge for personalised online shopping experiences.

The objective of this study is to develop an organizational and managerial toolkit for migrating retail EDI systems to a cloud-native architecture. To achieve this objective, two research tasks are set: first, to justify the governance stages of the migration process; second, to classify the technical risks associated with the transition to cloud-native EDI. The scientific novelty of the work lies in the fact that migration governance and migration risk are treated as a single managerial instrument rather than as separate concerns: each identified technical risk is mapped to a specific decision gate at which it is controlled, and to the organizational role accountable for that control. This distinguishes the proposed toolkit from existing cloud-migration frameworks, which either describe migration stages without linking them to a risk taxonomy, or assess risks without specifying the governance point at which each risk is resolved. The paper is organised according to the IMRAD structure: the Materials and Methods section sets out the object of study and the two methodological approaches applied; the Results and Discussion section presents the governance model and the risk classification matrix and compares them with published evidence; the Conclusion summarises the findings and outlines directions for further work.

Materials and Methods

This study is designed as applied methodological research. It does not test a statistical hypothesis; its purpose is to construct and justify a managerial instrument. The object of study is the process of migrating a retail EDI landscape from on-premises infrastructure to a cloud-native architecture. The subject of study is the organizational and managerial arrangements that govern this process. Two established methods are applied in sequence: the Stage-Gate project management approach, used to derive and justify the governance stages and their decision checkpoints, and qualitative risk analysis, used to identify and classify the technical risks of migration and to link each of them to a mitigation point within the resulting model. The empirical material consists of documented EDI migration projects in retail and logistics, together with vendor negotiation practice; published industry reports are used only as secondary evidence in the Discussion and are not treated as results of this study.

Theoretical grounding of the Stage-Gate approach

The Stage-Gate approach, formulated by Cooper, structures a complex project into a sequence of discrete stages, each separated from the next by a formal decision point, or gate [9]. Within each stage the project team performs a prescribed set of parallel activities that reduce a defined area of uncertainty. At each gate a designated decision-maker evaluates the deliverables of the preceding stage against pre-agreed criteria and issues one of a limited set of decisions: proceed, return for rework, hold, or terminate. Two properties of the approach are essential for the present context. First, gates are accountability points rather than progress reports: each gate has a named owner and an explicit pass criterion, so that responsibility for a decision cannot be diffused across the project team. Second, resources for the next stage are committed only after the gate is passed, which converts an open-ended technical programme into a sequence of bounded, reversible commitments [10].

The applicability of Stage-Gate to EDI migration follows from the structure of the migration problem itself. EDI migration is irreversible in its later phases, since trading partners cannot be repeatedly reconnected without commercial consequences; it involves several organizational functions whose obligations differ (IT, legal, procurement, security, operations); and its failure modes are latent, in that an incorrectly mapped message may be detected only after it has affected an order or an invoice. A stage-gated structure addresses all three properties: it forces the irreversible steps to be preceded by explicit verification, it assigns each verification to the function competent to perform it, and it prevents progression while a latent defect remains unresolved. Accordingly, the governance model presented in this paper adapts the Stage-Gate logic by defining five stages of EDI migration, a single mandatory gate for each stage, an explicit pass criterion for each gate, and a single accountable role per gate.

Qualitative risk analysis method

The second task is addressed through qualitative risk analysis, which is the appropriate method where risk probabilities cannot be estimated from a homogeneous historical dataset. This is the case in EDI migration: each retail landscape is a unique combination of legacy systems, partner profiles and contractual arrangements, so frequencies observed in one migration are not transferable to another. Qualitative analysis therefore characterises risks by source, mechanism and consequence rather than by numerical probability [11]. The procedure applied here follows four steps. First, risk identification: candidate risks were extracted from the documented migration projects and from the barriers reported in the literature on electronic data exchange and cloud migration [2], [7], [12]. Second, classification by source, separating technical-integration, regulatory, economic, organizational and contractual origins. Third, assessment of business consequence, in which each risk is expressed in terms of its effect on the retailer's operations rather than on the IT estate alone. Fourth, assignment of a mitigation point, in which each risk is mapped to the specific gate of the governance model at which it is controlled. The output of this procedure is the classification matrix presented in the Results and Discussion section.

The object of study is characterised as follows. Cloud-native EDI differs from legacy implementations in that processing is not bound to fixed servers in a single location. Message handling is decomposed into independent services — one receives inbound messages, another

converts them into the required EDI format, a third transmits them onward through APIs — so that the failure of one component does not halt the others, and capacity is added or withdrawn as transaction volume changes [3]. Integration with online storefronts and warehouse systems is achieved through APIs, which removes manual re-entry and the errors associated with it. These architectural properties define the technical environment within which the migration risks classified below arise; they are not themselves a result of the present study.

Results and Discussion

Construction of the governance model

Applying the Stage-Gate logic described above to the migration problem yields a governance model of five stages. Each stage corresponds to one area of uncertainty that must be closed before the next set of commitments is made: system assessment, vendor contract terms, data safety controls, phased rollout, and post-migration monitoring. For each stage the model specifies the activities to be completed, a single mandatory gate with an explicit pass criterion, and the organizational role accountable for the gate decision. The resulting model is presented in Table 1.

Table 1 sets out the five stages, their activities, gate criteria and accountable roles.

Table 1.

Stage-gated governance model for cloud-native EDI migration (compiled by the author)

Pillar	Main Activities	Approval Gate / Check Point	Responsibility
1. System Assessment	Document types, partners, volumes, mapping	Complete risk register signed off	IT governance team
2. Vendor Contract Rules	Pricing, SLAs, data ownership, penalties	Contract reviewed and signed	Legal + procurement
3. Data Safety Controls	Encryption, access rules, compliance checks	Security audit passed	Security officer
4. Phased Rollout	Pilot with one document type, side-by-side testing	Pilot results approved	Project manager
5. Post-Migration Monitoring	Monthly performance and cost reviews	3-month and 6-month reports accepted	Operations team

First, carry out a detailed assessment of the current environment. List every document type, every trading partner, and the exact daily message volumes. Map all connections to ERP or warehouse systems and note any outdated protocols. This step usually takes two to four weeks, but gives a clear picture of risks and costs.

Second, select the cloud provider and EDI platform carefully. Compare pricing, security features, and support for retail standards. In vendor negotiations, clear terms for data ownership, uptime guarantees, and penalties are essential requirements [4]. Ask for proof of earlier retail migrations that achieved zero downtime. Test two or three platforms side by side before deciding.

Third, carry out the migration in controlled phases. Start with one group of partners or one document type, such as purchase orders. Run the old and new systems together for two to four weeks. Many companies complete the full change without any service stop. The golf equipment manufacturer mentioned earlier followed this path and brought new-partner onboarding down to nine days or less [7].

Data security must stay in place at every step. Use encryption for messages in transit and at rest. Set strict access rules. The governance framework requires safety checks at every approval gate.

Fourth, train the team and update internal processes. Prepare short guides for the new monitoring tools and alerts. Run practice sessions so staff get used to real-time information. Adjust daily routines to take advantage of the fresh data.

Fifth, make adding new partners fast. Cloud platforms usually offer self-service portals and standard templates. Partners can connect with very little help from the internal team.

Finally, set up ongoing monitoring. Check performance every month, review costs, and adjust capacity when needed. The framework asks for short reports at three months and again at six months after go-live to confirm that all targets were met.

Applying the qualitative risk analysis procedure to the migration stages described above yields the classification presented in Table 2. Each row states a technical risk of EDI migration, expresses its consequence in business terms for the retailer, and identifies the gate of the proposed model at which the risk is controlled.

Table 2.

Classification of technical EDI migration risks, business implications and mitigation points within the proposed governance model (compiled by the author)

Technical risk of EDI migration	Business implication for the retailer	Mitigation point in the proposed governance model
Incompatibility of legacy ERP and warehouse interfaces with cloud message formats and protocols	Loss or misinterpretation of messages; order and stock errors reaching the customer	Stage 1 gate: full system map and signed-off risk register required before any live testing
Uncertain data residency and divergent privacy regimes across partner jurisdictions	Regulatory exposure; blocked cross-border flows; loss of partner confidence	Stage 3 gate: encryption in transit and at rest, documented residency register, security audit pass
Unbounded growth of consumption-based charges during demand peaks	Budget overrun in peak trading periods; erosion of the migration business case	Stage 5 gate: agreed budget envelope, monthly cost review, quarterly re-forecast
Partner connection failure during cut-over from the legacy system	Interrupted or lost order flow; partner attrition during the transition	Stage 4 gate: phased rollout by document type with parallel running until pilot results are approved
Internal capability gap in cloud monitoring, alerting and API operations	Slow incident response; message failures detected only after commercial impact	Stage 4 and 5 gates: completion of role-based training as a gate criterion; managed-service cover during stabilisation
Vendor lock-in through weak exit and data-portability provisions	Loss of commercial leverage; high switching cost at contract renewal	Stage 2 gate: data ownership, exit and portability clauses agreed before migration begins

The study produced two results. The first is the stage-gated governance model set out in Table 1. Its contribution is not the enumeration of migration activities, which are broadly known, but the binding of each activity group to a single mandatory gate, an explicit pass criterion and one accountable role. This converts a migration programme into a sequence of five bounded commitments, each of which can be audited independently: at any point in the process it is determinate which gate the project has passed, what evidence was required to pass it, and who authorised it.

The second result is the risk classification matrix in Table 2. Its contribution lies in the third column. Existing treatments of cloud migration risk describe risks and, separately, describe governance processes; the matrix links them, so that every identified technical risk resolves to a named gate at which it is controlled. The classification also reformulates each risk in terms of its business consequence for the retailer rather than its technical manifestation alone, which makes the risk register usable by the commercial and legal functions that own three of the five gates. Taken together, Tables 1 and 2 constitute the organizational and managerial toolkit stated as the objective of this study: the first defines where decisions are made, the second defines what must be resolved at each decision point.

The functional consequences of the migrated architecture, observed across the projects examined, are consistent with this structure. Invoice matching operates without manual input, with the system comparing amounts and raising only genuine discrepancies; three-way matching across purchase orders, invoices and shipment notices proceeds automatically. Shipment status is available in real time to retailer and customer alike, and EDI data flows directly into store systems so that stock records remain consistent. Where live shipment data is fed into recommendation systems, an event-driven configuration becomes possible, in which items shipping ahead of schedule can be surfaced to buyers in the relevant delivery area.

These functional changes shift the character of EDI within the retail organisation. Staff effort moves from routine reconciliation to exception handling, and the data generated by the migrated system becomes available for operational decisions rather than only for record-keeping.

In cross-border operations the same structure supports compliance with differing national requirements and absorbs seasonal demand growth without additional hardware procurement, provided that the residency and cost-control gates of the model are enforced.

Discussion

The evidence available in the published literature and in industry reporting is used here to assess the plausibility and practical utility of the proposed toolkit. It is external evidence and is not presented as a result of this study; none of the figures cited below were produced by the present research.

Industry reporting indicates that automated reconciliation in cloud EDI environments is associated with reductions in invoice matching errors of up to 90 percent, that partner onboarding times of one to nine days are achievable with self-service connection tooling against four to twelve weeks in on-premises configurations, and that first-year cost reductions in the range of 40 to 60 percent have been reported following migration [3], [4]. A documented migration by a large golf equipment manufacturer records continuity of service throughout transition and onboarding reduced to nine days or less, achieved by running legacy and cloud systems in parallel during testing [7].

Market analyses place the EDI software segment at 2.3–2.6 billion US dollars in 2025 with projected growth to 4.5–7 billion by 2030–2032, the cloud share increasing throughout. These figures indicate the scale of the potential benefit; they do not by themselves establish that the benefit is attributable to governance quality, which is the limitation the present toolkit addresses.

The proposed model can be positioned against existing work in three respects. Cooper's Stage-Gate formulation supplies the decision-gate logic but was developed for new product development, where termination at a gate is an acceptable outcome [9], [10]; in EDI migration termination after partner cut-over is not available, which is why the model concentrates its irreversible steps behind the third and fourth gates. Risk-analytic treatments of cloud migration establish that qualitative methods are appropriate where probability data are not transferable between cases, and provide taxonomies of migration risk [11], [12]; these taxonomies are organised by risk type rather than by the point of managerial control, and the matrix in Table 2 supplies that mapping. Existing cloud governance frameworks specify control domains for steady-state operation [5], [6], whereas the present model addresses the transition itself, which is bounded in time and has a different accountability structure. The barriers to electronic data exchange reported in supply chain research — legacy incompatibility, inconsistent standards and organisational resistance — correspond to the first, fourth and fifth rows of the classification, which supports the completeness of the risk set at the level of its principal categories [2], [7].

Three limitations should be stated. The toolkit is derived from migrations in retail and logistics and its transferability to other sectors with different partner structures has not been tested. The risk classification is qualitative, so it establishes the presence and control point of each risk but not its relative magnitude in a given landscape. And the model has been applied by its author, so independent application by other migration teams remains necessary to establish that the gate criteria are interpretable without the author's involvement.

Practical considerations in applying the model

The risks classified in Table 2 manifest in practice in the following ways, which also indicate how the corresponding gate criteria should be interpreted.

The most common problem is connecting older internal software to the new cloud system. Many retailers still use ERP or warehouse programs built years ago. These programs often work with different data formats or older protocols. Mapping and testing take extra time. If done too quickly, messages can be lost or read incorrectly [2]. The framework solves much of this by requiring a full system map early and approval gates before live testing starts.

Data security and compliance form another big concern. Retailers handle sensitive customer and supplier information. Privacy rules differ by country and change often [6]. Cloud platforms store data in various locations, so companies must know exactly where their information sits. Encryption in transit and at rest is necessary, but not enough by itself. Strict access controls and regular reviews are also required. Vendor agreements should include clear penalties if service levels are not met. The framework adds monthly safety checks to catch problems early.

Third, costs can rise faster than expected if they are not watched. Cloud services charge for actual usage, so big sales peaks can push bills higher [4]. The answer is to set clear budgets before migration and review them every three months after go-live. The ongoing monitoring pillar makes this a normal part of operations.

Fourth, some partners still need guidance during onboarding, even with self-service tools [7]. Standard templates and short training materials usually take nine days or less.

Fifth, the internal team often needs time to learn new skills in cloud monitoring, alerts, and API work. Short guides and practice sessions help close the gap. Some companies use managed services for the first six months while the team builds confidence.

Finally, depending too much on one vendor can create problems later [5]. Strong contract terms on exit procedures and data ownership, agreed at the beginning, reduce this risk.

In the coming years, simple artificial intelligence tools will probably improve matching and forecasting inside EDI systems [8]. These tools will strengthen personalisation, but they will also need extra checks on accuracy. The governance framework can be extended to cover them when the time comes.

The challenges are significant, yet they become manageable with a structured governance approach. The five-pillar approach turns potential weak points into controlled steps.

Conclusion

Cloud-native EDI removes many of the constraints that on-premises systems placed on retailers. Companies gain real speed, greater scale, and lower costs. When migration follows the proposed governance framework. The shift eliminates legacy infrastructure barriers and lets retailers process millions of transactions daily with zero downtime and full scalability for global marketplaces.

The scientific contribution of the work lies in this mapping: migration governance and migration risk are treated as one instrument rather than two, so that the question 'who resolves this risk, and at which point' has a determinate answer for every risk in the set.

For retailers preparing for tomorrow's market, cloud-native EDI is more than a technical upgrade. It becomes a competitive advantage. Stores that make the move can grow faster in global markets, reduce errors, and deliver the fast and personal service that online buyers now expect. Automation of key tasks supplies correct information at the right moment, which supports better stock decisions, quicker deliveries, and stronger customer relationships.

For practice, it is recommended that retailers complete the stage-one assessment and sign off the risk register before entering vendor negotiations, since the contractual gate depends on knowing which risks must be allocated contractually; that progress be measured against the gate criteria rather than against elapsed time; and that the three- and six-month post-migration reviews be treated as formal gates rather than status reports.

Further work should test the transferability of the toolkit to sectors with different partner structures, and examine whether the gate criteria can be applied consistently by migration teams other than the author's. The extension of the classification to risks arising from the introduction of machine learning components into EDI matching and forecasting is a further direction, since such components introduce accuracy-assurance requirements that the present five gates do not yet address.

References

1. Klapita V. Implementation of electronic data interchange as a method of communication between customers and transport company // *Transportation Research Procedia*. – 2021. – Vol. 53.
2. Werner-Lewandowska K., Kolinski A., Golinska-Dawson P. Barriers to electronic data exchange in the supply chain: results from empirical study // *LogForum*. – 2023. – Vol. 19, No. 1.
3. Mannava S.K. Optimizing EDI integration: a guide to cloud-based systems and business efficiency // *International Journal of Computer Engineering and Technology*. – 2025. – Vol. 16, No. 1.
4. Hosseini Shirvani M., Amin G.R., Babaeikiadehi S. A decision framework for cloud migration: a hybrid approach // *IET Software*. – 2022. – Vol. 16, No. 6.
5. Folorunso A., Adewa A., Babalola O., Nwatu C.E. A governance framework model for cloud computing: role of AI, security, compliance, and management // *World Journal of Advanced Research and Reviews*. – 1982. – Vol. 24, No. 2.
6. Mazula D., Lamprecht C. Redefining enterprise cloud technology governance // *ISACA Journal*. – 2023. – Vol. 3.
7. Jain M. Analysis of electronic data interchange (EDI) adoption challenges and best practices in retail supply chains // *Journal of Global Research in Mathematical Archives*. – 2025. – Vol. 12, No. 12.
8. El Fellah K., El Azami I., El Makrani A. A comparative analysis of blockchain and electronic data interchange (EDI) in supply chain: identifying strengths, weaknesses, and synergies // *Journal of Autonomous Intelligence*. – 2024. – Vol. 7, No. 5. – Art. 1481.
9. Cooper R.G. Perspective: The Stage-Gate idea-to-launch process – update, what's new, and NexGen systems // *Journal of Product Innovation Management*. – 2008. – Vol. 25, No. 3.
10. Cooper R.G. What's next? After Stage-Gate // *Research-Technology Management*. – 2014. – Vol. 57, No. 1.
11. Zeng W., Yan W., Simpson E., Molina-Jimenez C. Quantitative risk assessment for cloud-based software migration processes // *Concurrency and Computation: Practice and Experience*. – 2025. – Vol. 37, No. 4.
12. Valladares S., Ticona W. Information technology risk management due to the migration of infrastructure to cloud services: a systematic review // *Lecture Notes in Networks and Systems*. – 2025. – Vol. 1559.