CONCEPTUAL PRINCIPLES OF REGULATORY AND LEGAL SUPPORT OF MANAGEMENT IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF SOCIETY

Uliana Nikonenko[1]

DOI: https://doi.org/10.30525/978-9934-26-651-5-35

Abstract. This study addresses the conceptual foundations and practical mechanisms of normative and legal support for management in the context of society's digital transformation, emphasizing that legality and managerial effectiveness must be designed as one integrated governance system rather than treated as separate tracks. It explains how multi level regulation, fundamental rights and principles, sector specific obligations, supervisory expectations, contractual allocation of duties, internal policies, and technical assurance practices collectively shape lawful and resilient digital operating models. The analysis links core management functions, including planning, process design, human resource governance, financial and operational control, compliance, and incident response, to embedded safeguards and evidence producing workflows that enable accountability in audits and disputes. Special attention is given to high impact risk areas such as personal data governance, cybersecurity and continuity, electronic records validity, vendor and outsourcing exposure, remote work and workplace fairness, and algorithm supported decision making, including technologies based on artificial intelligence, where transparency, explainability, non discrimination, and human oversight become decisive. The results highlight that successful digital transformation depends on clear roles, decision rights, escalation pathways, and continuous control operation, supported by consistent documentation and measurable evidence, which together reduce legal uncertainty, strengthen stakeholder trust, and improve organizational resilience while preserving speed and innovation capacity in a rapidly changing digital environment.

[1] Doctor of Economics, Professor,
Department of Management and Marketing in Publishing and Printing
Lviv Polytechnic National University, Ukraine
ORCID: https://orcid.org/0000-0002-6015-6248

Introduction

The modern digital transformation of society is significantly changing the way organizations set goals, make management decisions, and build interaction with stakeholders in the internal and external environment. Management increasingly relies on data, electronic processes, remote work formats, automation, and solutions based on applied digital technologies, so the legal field that was created for paper procedures and traditional organizational models appears to be insufficiently coordinated with new practices. The relevance of the topic is due to the fact that without clear regulatory and legal support, managers and employees face increased uncertainty, and the risks of errors in organizing processes, protecting rights, and fulfilling duties often grow faster than the organization's ability to identify and minimize them in a timely manner. At the same time, the digitalization of management directly affects the legitimacy of management actions and the demonstrability of management decisions. Electronic documents, electronic signatures, electronic registers, digital communication channels, remote meetings and automated workflows require clear rules on authority, responsibility, storage and reproduction of information, as well as on the legal force of electronic actions. At the same time, in many organizations, practice is ahead of regulatory clarifications, which leads to conflicts between internal policies, regulatory requirements and contractual obligations. The conceptual foundations of legal management support should form the basis for harmonizing management procedures with legal principles so that digital processes not only increase efficiency, but also remain legitimate and reproducible in the event of disputes and audits. The issue of data as a key management resource is gaining special importance, because analytics, performance monitoring, client profiles, HR systems and financial platforms work on arrays of personal and commercial information. At the same time, requirements for the protection of personal data, confidentiality, trade secrets, archiving, access and access restrictions require clear integration into management processes, rather than adding them “after the fact”. At the same time, cybersecurity is becoming a legal and managerial category at the same time, since incidents affect business continuity, reputation and financial results, and also entail legal consequences for the organization and officials. That is why the relevance of the topic lies in the formation of such a direction of regulatory and legal

support that provides management with clear rules for prevention, response and responsibility in the digital environment.

The importance of the study is enhanced by the spread of algorithmic approaches to decision-making, in particular in personnel selection, performance evaluation, lending, pricing, compliance control and risk management, including the use of technologies based on artificial intelligence. At the same time, such approaches give rise to new challenges regarding transparency, non-discrimination, explainability of decisions, liability for algorithm errors and the rights of employees and customers to fair treatment. At the same time, the importance of management ethics as a practical extension of law is growing, because even formally legal digital practices may contradict public expectations and corporate values. The conceptual principles of regulatory and legal support for management should determine how to combine innovation and the speed of digital change with appropriate guarantees of human rights, safe working conditions and trust in organizations. Thus, the relevance and importance of the topic is determined by the need to systematically rethink the regulatory and legal support for management in the context of the digital transformation of society so that it does not lag behind real management practice. At the same time, we are not talking about fragmentary amendments, but about a holistic concept that describes the principles, priorities and mechanisms for harmonizing legal norms with management functions, from planning and organization to control and responsibility. At the same time, such conceptualization provides the basis for developing internal policies of organizations, improving the quality of regulatory decisions of state authorities and forming a stable environment for innovation. As a result, the topic is key to ensuring the legitimacy, sustainability and competitiveness of organizations in the digital environment, where legal certainty appears as one of the basic conditions for effective management.

1. Theoretical and methodological foundations of regulatory and legal support for management in the context of digital transformation of society

Regulatory and legal support for management in the context of digital transformation of society is a set of legal norms, principles and procedures that determine the boundaries and order of management activities, as

well as guarantee the legitimacy of management decisions in a situation where key processes of the organization are transferred to electronic format. At the same time, digital transformation is not limited to the implementation of individual programs or communication channels, it changes the very nature of management, since decisions are made faster, based on data, depend on access to information resources and are often implemented through automated workflows. At the same time, classic management functions, in particular planning, organization, coordination, motivation, control, are preserved, but acquire new forms. Planning is increasingly based on forecasting and modeling, organization appears as the construction of processes in a digital environment, and control becomes continuous through digital traces, event logs and analytics systems. That is why the theoretical formation of the basis of the topic requires the coordination of two planes, the managerial one, where efficiency and effectiveness are important, and the legal one, where legality, certainty and protection of the rights of the participants in the relationship are key. In the absence of such coordination, the organization risks finding itself in a situation where technologically modernized processes remain legally vulnerable, and therefore, their stability, provability and reproducibility in the event of disputes becomes limited [1-3].

A key element of the conceptual principles is a clear definition of the object and subject of regulatory and legal support for management. The object is managerial relations in the internal and external environment of the organization, which arise during the creation, processing, transmission, storage and use of information, as well as during the organization of work, interaction with counterparties, clients, employees, state authorities and society. The subject is legal mechanisms that regulate digital processes and ensure a balance between managerial expediency and legal guarantees. At the same time, it is important not to confuse legal support with technical regulations, because the law establishes mandatory rules of conduct, grounds for liability, procedures for confirming facts and protecting rights, while technical standards determine technological parameters. At the same time, in the digital environment, the line between them becomes thinner, since technical solutions often become a way to implement legal requirements. For example, the legal force of an electronic document depends not only on the content, but also on how the signer's identification, file integrity, date and time of creation, and the ability to verify authenticity are ensured.

Thus, within the theoretical and methodological framework, it is necessary to consider regulatory and legal support as a system where legal norms, internal organization policies, and technological mechanisms mutually complement each other, forming a manageable and legally sustainable direction of digital transformation.

The principles on which the regulatory and legal support of management is based acquire special practical importance in the digital environment, since they help to make decisions in conditions where specific norms lag behind technological changes or contain conflicts. The basic principles include legality, legal certainty, proportionality, accountability, non-discrimination, protection of personal data, confidentiality, business continuity, good faith and fairness. At the same time, these principles must be translated into the management language of processes, indicators and responsibility. At the same time, the principle of data minimization appears in digital transformation, when the organization collects only the data that is really necessary to achieve the goal and stores it no longer than is justified. At the same time, the principle of transparency is strengthened, because decisions made on the basis of data or through automation must be understandable to the employee, client or counterparty, at least in the part that concerns their rights and obligations. The principle of responsibility plays a special role, because in the digital environment, an error can scale instantly, for example, due to incorrect access settings or due to an incorrectly defined business process that is automatically applied to thousands of operations. Thus, the conceptual framework should form such rules under which technological speed does not destroy the legal quality of management, but, on the contrary, provides an opportunity to strengthen compliance with the law through controlled processes and recording digital traces.

Table 1 presents the layered nature of normative and legal support for management during digital transformation. The central idea is that legality in digital operating practice does not come from a single document or a single regulator, it emerges from an aligned system of layers that reinforce each other. At the highest level, fundamental rights and general legal principles set boundaries that management cannot bypass even when technology enables faster decisions and broader data use. Sector and functional legislation then translates those principles into concrete obligations that affect electronic documents, delegation of authority, record retention, labor relations, and information security duties.

Table 1

Layers of normative and legal support for management during digital transformation

Layer and scope	What it regulates for management practice	Typical deliverables inside the organization	Practical value and common failure points
1	2	3	4
Fundamental rights and general legal principles	It sets non negotiable boundaries for any managerial action in a digital setting, including privacy, fairness, protection of personal data, freedom of contract, and access to remedies. It also shapes how proportionality and accountability should appear in day to day decisions when digital tools accelerate operations	A concise internal statement of governance principles that is referenced in policies, procurement templates, and training materials. A decision record format that forces managers to justify necessity, proportionality, and expected impact on people and partners	It provides legitimacy and predictability, especially when detailed rules lag behind technology. A frequent weakness appears when principles are stated in documents but are not translated into process steps and measurable responsibilities, which later makes audits and dispute resolution harder
Sector and functional legislation affecting management	It defines concrete obligations for electronic documents, electronic signature, record retention, consumer and competition rules, labor relations, occupational safety, and information security duties. It shapes how management can design processes, delegate authority, and rely on digital evidence in disputes	A compliance register that maps each obligation to a business process owner, a control step, and evidence artifacts. Operating procedures for electronic document flows, retention schedules, and legally valid approvals in digital systems	It reduces legal risk and operational uncertainty by turning general requirements into enforceable routines. A common failure point is partial implementation, where a new digital process is launched, but the matching legal basis, records, and retention controls are missing

(End of Table 1)

1	2	3	4
Regulatory guidance and supervisory expectations	It clarifies how regulators interpret ambiguous rules, what they expect in audits, and what constitutes due diligence in areas such as cybersecurity, personal data, and incident reporting. It often influences how fast management must respond, what must be documented, and how communication with stakeholders should be handled	Regulatory monitoring notes, internal guidance summaries, audit readiness checklists, and reporting playbooks for incidents and compliance issues. Training modules for managers that explain how to act during an inspection or a complaint	It improves resilience because management knows what to do before a crisis happens. A typical weakness is treating guidance as optional and ignoring it until an incident occurs, which may lead to harsher supervisory reactions due to weak evidence of preparedness
Contractual layer with partners and technology providers	It allocates responsibilities and liabilities across the supply chain, including confidentiality, data processing, security measures, service continuity, breach notification duties, and rights to audit. It shapes managerial control over outsourced processes and cloud services that handle critical data and operations	Standard contract clauses, data processing agreements where relevant, service level agreements, exit plans, and vendor security questionnaires. A documented approval route that links procurement to legal review and security assessment	It protects the organization when external vendors process data or run critical services. A common failure point is signing contracts that promise strong safeguards on paper, while actual technical configurations and monitoring do not match, which later weakens enforceability and recovery

Source: Formed by the author

Regulatory guidance adds an interpretative layer that shapes what supervisory bodies consider reasonable due diligence. Contracts with partners and providers allocate responsibilities across the supply chain, which becomes decisive when key processes and data move to external platforms. Internal policies and procedures convert external requirements

into daily managerial routines, while technical standards and assurance practices support credibility by showing that controls are designed and operated systematically.

A separate component of the theoretical basis is the multi-level legal regulation of management in the context of digital transformation. At the top level are constitutional guarantees of human rights, in particular the right to privacy, protection of personal data, freedom of enterprise, the right to work and safe working conditions, as well as guarantees of judicial protection. Next are laws and by-laws that define the rules of electronic document flow, electronic identification, information storage, labor relations, labor protection, information protection, contract law, and liability of officials [4-5]. Along with this, the supranational level becomes important when the organization works with partners or clients from other countries, or processes data according to the rules operating in the international economic space. At the same time, a key area that cannot be underestimated is the organization's internal policies, including provisions on access to information systems, rules for working with personal data, cybersecurity policies, remote work regulations, incident management procedures, and rules for storing electronic documents. It is internal policies that transform general legal norms into specific management procedures, identify responsible persons and control mechanisms. Thus, conceptual principles should explain how to coordinate these levels so that there is no gap between what the law requires and how management actually works in the digital environment. An important methodological issue is the ratio of management risk and legal risk in digital transformation. Management risk manifests itself through the probability of failure to achieve goals, loss of efficiency, process disruptions, planning errors, and a decline in service quality. Legal risk manifests itself through violations of the law, penalties, litigation, loss of evidence, reputational consequences, and liability of officials. At the same time, in the digital environment, these risks are intertwined, as a technological error can easily become a legal problem. For example, insufficient control of access to the system can lead to a leak of personal data, which simultaneously causes operational losses and legal consequences. At the same time, risk can also arise from excessive control, when an organization applies employee monitoring tools without proper legal basis or without proportionality, which undermines trust and

creates conflict in labor relations. That is why the methodology of the topic should include risk assessment as a continuous management process that is integrated into legal support, and does not exist separately. Therefore, this means that the conceptual framework should define the rules for identifying risks, documenting them, determining those responsible, the procedure for responding and ways to confirm the actions taken. This approach provides an opportunity to transform law from a reactive tool for punishment into a proactive tool for managing the sustainability of digital transformation. A significant challenge that needs to be addressed at the theoretical level is the algorithmization of management decisions and the use of AI-based technologies in business processes. In the digital environment, more and more decisions are made based on recommendations from systems that analyze large data sets, offer ratings, risk profiles, predictive indicators, or automatically apply rules to typical situations. At the same time, management cannot shift responsibility to the program, even if it technically performed the action, since legal responsibility for the consequences remains with the organization and authorized persons. At the same time, issues of explainability arise, i.e. the ability to justify why the decision was made, as well as the issue of non-discrimination, when algorithmic models can reproduce data distortions and create systemic injustices against certain groups. At the same time, the issue of evidence becomes important, because in judicial or control procedures it is necessary to recreate the decision-making chain, show data sources, rule settings, authorizations, access protocols, and changes in model versions. Thus, the conceptual framework for regulatory management should describe the principles of human control, the limits of automation, the requirements for documenting algorithmic decisions, the procedure for auditing models, the rules for ethical and lawful use of data. At the same time, they should provide management with a clear direction on how to combine innovation and the speed of digital transformation with guarantees of human rights, workers' rights, consumer rights and the stability of contractual relations.

Effective implementation of regulatory and legal support for management in a digital environment requires a holistic model that combines legal requirements, management functions and real-world process settings in information systems. At the same time, an organization cannot limit itself to creating separate documents, since the key value is that the rules work

as part of daily operational activities, leave a verifiable trace and provide management with the opportunity to make decisions quickly but legally. At the same time, digital transformation appears as a continuous process, so the implementation model should not involve a one-time setting, but a cycle of constant review of rules, updating procedures, training personnel and adjusting controls taking into account incidents and changes in the internal and external environment. Thus, the subject of management attention is not only compliance, but also the ability of the legal and management system to maintain stability, trust and manageability in a situation of accelerating technological change.

Table 2 connects management functions with legal and ethical obligations, then translates them into process design practices and evidence expectations. The value of this alignment is practical, because management functions such as planning, organizing workflows, managing people, controlling finances, and responding to incidents are where legality is either protected or violated in daily operations. Digital transformation accelerates these functions through data driven decision support, automated approvals, remote collaboration, and continuous monitoring, which increases both capability and exposure. The table therefore emphasizes embedded governance, meaning legal requirements must be built into how initiatives are approved, how workflows are configured, how authority is delegated, and how records are retained. For example, strategic planning in a digital setting must include necessity and proportionality reasoning for data use, not as a legal afterthought but as a managerial decision discipline that clarifies purpose, limits, and safeguards.

At the same time, the inventory often reveals that the organization has parallel communication channels, duplication of storage, inconsistent rules for document retention, and blurred lines of responsibility between departments. At the same time, it is important to describe the chains of creation, approval, signing, storage, and access to electronic documents, separately recording those stages where authority is required, where there is a need to confirm time and integrity, and where conflicts of interest are possible. At the same time, it is necessary to determine the categories, processing purposes, legal grounds, retention periods, the circle of persons with access, and a list of external contractors who have access to the information for the data.

Table 2

Management functions aligned with legal requirement s and digital operating practices

Management function in a digital organization	Core legal and ethical obligations that must be embedded	Process design and control practices	Evidence that should exist for audits and disputes
1	2	3	4
Strategic planning and goal setting	Management must justify why data collection, monitoring, and automation are necessary for the stated purpose, and must avoid excessive intrusiveness. It should also anticipate impacts on employees, customers, and partners, and prevent unfair outcomes	Create a decision procedure that requires legal basis, proportionality reasoning, and stakeholder impact review before digital initiatives are approved. Use a consistent template that forces clarity on data categories, retention, and accountability	Approved business case documents, impact assessments where relevant, records of stakeholder consultations, and board or executive approvals. A traceable chain that shows who decided, on what grounds, and with what safeguards
Organizing processes and digital workflows	Management must ensure legal validity of electronic approvals, integrity of records, and proper delegation of authority. It must also preserve reliable records for retention and later verification	Map each process step to a legal requirement, assign process owners, and embed controls directly in systems. Configure role based access, workflow approvals, and immutable logs for critical actions	Process maps, delegation matrices, system configuration records, audit logs, and retention schedules. Evidence that the process works as designed, including samples of real executed workflows
Human resources and the future of work	Management must respect labor rights, privacy boundaries, fairness in evaluation, and transparency when using monitoring or algorithmic support tools. It must also ensure safe working conditions for remote and hybrid models	Implement clear remote work policies, monitoring limits, and grievance channels. Ensure algorithm supported decisions have human review steps, explainability expectations, and documented non discrimination checks	HR policies, employee notices, training records, consent or legal basis records where required, and documented reviews of algorithmic tools. Records of complaints and resolution steps show practical enforcement

(End of Table 2)

1	2	3	4
Financial and operational control	Management must ensure accuracy, traceability, fraud prevention, and lawful processing of financial and transactional data. It must also prevent unauthorized changes to critical master data and payment instructions	Use segregation of duties in digital systems, dual approvals for high risk changes, and continuous monitoring of anomalies. Implement change control for financial configurations and maintain strong vendor management for payment related services	Approval records, reconciliations, exception reports, logs of master data changes, and incident records tied to corrective actions. Evidence should show consistent operation, not only policy existence
Compliance and internal control	Management must maintain ongoing conformity, not a one time compliance event, and must document due diligence. It must also handle complaints, audits, and regulatory interactions with consistent procedures	Maintain a compliance register linked to processes, test controls periodically, and track remediation to closure. Establish an escalation route and a clear rule set for what triggers legal review and external notification	Control testing results, remediation plans with owners and deadlines, audit reports, and correspondence logs. A complete trail of actions demonstrates accountability and good faith behavior

Source: Formed by the author

Such a description forms the basis for the next steps, since without it, policies and regulations remain general and do not ensure the manageability of digital processes. At the same time, it is important that the rules have unambiguous definitions, clear conditions of application, and a clear procedure for recording the actions performed, since it is these elements that will later provide evidence in audits and disputes. At the same time, special attention is required for processes where an error scales instantly, for example, payments, changes in counterparty details, assignment of access rights, deletion or modification of data, publication of messages for clients, launch of automated scripts in systems. At the same time, it is appropriate

to implement the principle of separation of powers, when critical actions require confirmation by another authorized person, as well as the principle of minimally necessary access, when each employee has only those rights that are necessary to perform specific functions. Thus, legal regulation appears not as a text, but as a practical mechanism that is built into digital processes and supported by system settings [6-7]. At the same time, control should be risk-oriented, that is, focused on those processes and data where the consequences of errors are most significant for the rights and legitimate interests of people, for the financial stability of the organization, for the reputation and continuity of business. At the same time, control should include checking the implementation of procedures, analyzing event logs, regularly reviewing access, assessing the implementation of document retention periods, assessing the quality of staff training and analyzing recurring deviations. At the same time, it is important to implement a corrective action mechanism, where each identified violation has an owner, a deadline for elimination and confirmation of implementation, and the final results are used to update policies and settings in systems. Thus, the organization receives a managed process of continuous improvement, where law and management mutually support each other through the discipline of control and transparent accountability.

This includes not only cyberattacks, but also any event that results in data integrity violations, unauthorized access, loss of service availability, erroneous automation, or misuse of information. At the same time, the organization should have predefined roles, escalation procedures, decision-making rules, procedures for preserving evidence, and procedures for interacting with counterparties, including service providers who may hold key technical logs and backups. At the same time, external communication rules are needed to ensure that messages to customers and partners are accurate, consistent, and do not create additional legal risks. Thus, incident management becomes a component of legitimate management, where the speed of response is combined with the discipline of documentation and protection of the rights of persons who may be affected by the incident. At the same time, the organization must determine which decisions can be fully automated, which can be partially automated, and which require mandatory confirmation by an authorized person, in particular in areas that significantly affect the rights of employees, customers or partners. At the

same time, rules are needed for the data used to train and adjust models, including data quality assessment, bias control, versioning and fixing changes, so that at any time it is possible to reproduce why the decision was made as it was. At the same time, it is advisable to create an appeal procedure when a person can request a review, receive a clear explanation and have the error corrected. Thus, the organization combines innovation with legal guarantees, and digital transformation maintains the trust and predictability that are crucial for sustainable development.

A sustainable approach to normative and legal support in management requires a roadmap that connects strategy, governance, process design, and technology configuration into one coordinated trajectory. Leadership should treat legality, accountability, and stakeholder trust as core design requirements for transformation, alongside efficiency and speed. Such a roadmap begins by clarifying the organization's risk appetite and ethical boundaries, then translating those boundaries into operational rules that managers can apply without improvisation. The overall objective is to ensure that every high impact digital change, including new data use cases, new platforms, and automation of decisions, is launched with a defensible legal basis, clear responsibility, and reliable evidence generation embedded into daily workflows. A first recommendation focuses on building a unified governance architecture that eliminates responsibility gaps and reduces decision ambiguity. Governance should define who owns each critical process, who approves exceptions, who validates legal basis for data use, and who has authority to stop deployments when safeguards are insufficient. Escalation pathways should be explicit and practiced, covering privacy concerns, cybersecurity vulnerabilities, contract deviations, and algorithm supported decisions that can materially affect employees, customers, or partners. Governance outputs should include a compliance register linked to process owners, an approval template for transformation initiatives that requires proportionality and impact reasoning, and a recurring reporting routine that shows not only policy adoption, but also control operation and remediation closure. A second recommendation addresses process and evidence design, because defensibility in audits and disputes depends on traceability rather than declarations. Organizations should map end to end workflows for legally relevant activities, such as electronic approvals, delegation of authority, record retention, access provisioning, master data

changes, incident response decisions, and external communications during crises. Each mapped workflow should include control points that are enforced by system settings where possible, for example role based access, segregation of duties, immutable logs for critical events, and automated retention enforcement. Evidence requirements should be defined at the same time as process design, ensuring that logs, approvals, version histories, and decision records are retrievable, complete, and consistent across platforms, including outsourced services.

Vendor onboarding should include legal and security due diligence that is tied to concrete acceptance criteria, rather than generic questionnaires. Contracts should clearly allocate responsibilities for confidentiality, security measures, incident notification timing, cooperation in evidence preservation, service continuity, and exit readiness. Ongoing vendor oversight should verify that contractual safeguards are reflected in real operations, including access governance, monitoring practices, and incident handling drills. A workable exit plan should be maintained and tested, so that dependency on a single provider does not become a structural legal and operational risk. Training should be role specific and connected to real workflows, so employees understand what actions are permitted, what evidence they are expected to leave, and why shortcuts create legal and operational exposure. Management should reinforce consistent consequences for violations and consistent support for reporting concerns, so that employees do not feel pressure to bypass procedures for speed. Remote and hybrid work rules should specify monitoring boundaries, transparency expectations, retention limits for employee related data, and an accessible grievance route. Cultural maturity grows when employees see that governance improves workflows and reduces uncertainty, rather than adding paperwork.

The organization should define decision categories that require mandatory human oversight, especially for high impact outcomes such as hiring, performance assessment, pricing, eligibility determinations, and compliance screening. Model governance should include documentation of purpose and limitations, version control, approval records for deployment changes, stability and bias assessments, and an appeal procedure that allows affected persons to request review and obtain an understandable explanation. Data governance for model development should ensure lawful

basis, data minimization, retention discipline, and controlled access, while also maintaining a clear record of what data sources were used and under what safeguards.

2. Practical mechanisms and tools for regulatory and legal support of management in the context of digital transformation of society

The practical disclosure of the topic begins with the fact that regulatory and legal support should be built into everyday management, and not exist separately in the form of formal documents. The organization is faced with the need to translate legal requirements into specific management procedures that work in the internal and external environment, give a predictable result and leave an evidentiary trace. At the same time, digital transformation changes the pace of decision-making, so legal verification cannot be just a final stop, it should be part of planning, process design, definition of powers and control points. At the same time, it is important to form a unified approach to what is considered a regulatory requirement in the organization, what is an internal standard, and what is a recommendation, since mixing these levels often creates management conflicts and increases liability risks. Thus, the practical vector of the section is to transform the law into a set of understandable management rules that support efficiency, ensure legitimacy and build trust in digital processes [8-10].

Table 3 focuses on risk areas that typically become critical during digital transformation, then links them to triggers, controls, and evidence artifacts. The purpose is to move from abstract risk awareness to operational readiness. Each risk area is framed as a predictable pattern, meaning organizations can anticipate when risk rises, such as during cloud migration, expansion of analytics, integration of data sources, increased reliance on vendors, and rapid software releases. The table shows that many incidents originate from normal transformation activity rather than malicious intent, for example purpose creep in data use, weak access hygiene in remote work, unclear rules for electronic records validity, or contractual misalignment with vendor operations. That framing is important because it encourages management to treat legality as part of transformation design, not as a separate compliance project that starts after deployment.

Table 3

Key risk areas for normative and legal support, triggers, controls, and evidence

Risk area	Typical triggers during digital transformation	Preventive and corrective controls	Evidence artifacts that prove due diligence
1	2	3	4
Personal data and privacy risk	Expansion of analytics, customer profiling, employee monitoring, new digital channels, and integration of multiple data sources. Purpose creep, where data starts being used beyond the original goal, is a recurring trigger	Define lawful basis for processing, limit data to necessity, and apply retention rules that are enforced by systems. Establish access control, transparency notices, and a procedure for data subject requests and complaints	Data inventories, processing registers, notices provided to individuals, request handling records, and access logs. Proof that retention and deletion rules are applied consistently is especially important
Cybersecurity and service continuity risk	Migration to cloud services, remote access growth, increased dependence on third party vendors, and faster software releases. Weak access hygiene and untested incident procedures commonly trigger major failures	Implement strong identity and access management, multi factor authentication where appropriate, monitoring, patch management, and secure configuration baselines. Maintain tested backup and recovery procedures, and run incident response exercises with documented outcomes	Security policies and configurations, monitoring reports, vulnerability management records, exercise reports, and incident tickets with timelines. Evidence should show continuous operation of controls, not only initial setup
Electronic records validity and evidentiary risk	Replacement of paper approvals with digital workflows, unclear rules for electronic signature usage, inconsistent retention, and uncontrolled system changes. Later disputes may expose gaps in authenticity and integrity	Adopt documented rules for electronic documents, define what constitutes valid approval, enforce immutable logs, and implement retention schedules with periodic checks. Use change management controls for systems that store legally relevant records	Electronic approval records, signature verification logs if applicable, retention reports, audit trails, and change management documentation. Samples of records should be retrievable quickly and reliably

(End of Table 3)

1	2	3	4
Vendor and outsourcing legal risk	Use of external providers for hosting, development, support, and data processing, often across borders. Misalignment between contract terms and actual operations is a frequent trigger, especially around incident notification and security responsibilities	Perform vendor due diligence, contractually require security measures and audit rights, define incident cooperation duties, and create exit plans. Monitor vendor performance, security posture, and compliance with contractual obligations over time	Vendor risk assessments, signed agreements, service reports, audit results, incident communication logs, and exit readiness documentation. Evidence should show active governance, not only procurement stage checks

Source: Formed by the author

The first tool for implementing such an approach is a system of internal policies, procedures and regulations that detail legislative norms for specific business processes. These include regulations for electronic document management, policies for electronic identification and signature, procedures for maintaining electronic archives, rules for accessing information systems, procedures for granting and revoking access rights, as well as requirements for event logging and log storage. At the same time, documents are needed that determine how the organization works with personal data, how it records the legal grounds for processing, how it configures storage periods, how it ensures the rights of data subjects and how it confirms the execution of requests. At the same time, the consistency of internal rules with contractual work becomes key, since cloud service providers, system support contractors, outsourcing teams and consultants gain access to data and processes, and therefore, contractual terms should include requirements for confidentiality, security, liability, the procedure for reporting incidents and the conditions for returning or destroying data after the end of cooperation. Such a package of internal rules provides an opportunity to make the management of digital processes not only convenient, but also legally defined. The second practical component is the organization of responsibility and accountability in the digital environment, when each critical process has a process owner responsible for compliance with the rules, and a clear escalation trajectory in the event of violations or incidents. In this context, it is important not

infrequently to move from personal responsibility in the form of formal job descriptions to process responsibility, where it is determined who makes the decision, who approves, who executes, who controls, and how this is confirmed in the system. At the same time, it is appropriate to implement the principle of separation of powers so that critical operations, such as changing access rights, approving payments, changing counterparty details, deleting data, are not performed alone without recording a second control. At the same time, digital transformation provides mechanisms that can strengthen legitimacy, such as automatic document routing rules, version control, the inability to edit approved records without leaving a trace, and approval protocols. Thus, the formation of the basis of legitimacy becomes operational, that is, it is built into processes and reflected in digital traces that can be verified.

The third component is risk management and compliance control, where law is combined with compliance and internal control. In practice, this means regularly assessing legal risks that arise from process changes, the introduction of new platforms, integration with registries, the launch of remote working modes, the use of biometric or geolocation data, as well as the involvement of external contractors. At the same time, efficiency is provided by an approach where each digital transformation initiative undergoes an assessment of legal consequences at the design stage, and not after launch. At the same time, control should include access audits, audit of procedure implementation, selective verification of compliance of contracts with actual practice, incident analysis and corrective actions. It is important that control does not turn into bureaucracy, it should be proportionate, risk-oriented and provide management with information to improve processes. At the same time, documenting control results becomes critical, because it is this that confirms management's due diligence and reduces the likelihood of claims from regulators and counterparties. The fourth component is the legal support of cybersecurity and incident response as a management process, which requires not only technical actions, but also legally correct procedures. Practice shows that an incident often develops quickly, so the organization must have a predetermined procedure for classifying events, making decisions on isolating systems, preserving evidence, communicating with customers and partners, as well as interacting with government authorities, if required by law. Along with this, important are

procedures that determine who is authorized to make public statements, how notifications are agreed, what deadlines apply, and how the fact of notification is recorded. At the same time, from a legal perspective, preserving the integrity of evidence becomes critical, since without the correct protocol for collecting and storing digital traces, the organization may lose the opportunity to protect its rights in a dispute or prove the good faith of its actions. At the same time, cybersecurity should be linked to labor rules, because negligence or violation of access rules by an employee should have clear consequences, and training and regular briefings should be designed in such a way that they can be confirmed. The organization should set boundaries for where automation is allowed, where mandatory human confirmation is required, and how explainability of decisions for the employee, client or counterparty is ensured. At the same time, it is necessary to define rules for working with data for training models, data quality requirements, a procedure for checking for bias, audit procedures, as well as rules for recording model versions and changes in settings. At the same time, it is important to form appeal mechanisms where an individual can ask questions about a decision, receive a clear explanation and seek a review in case of an error. This approach provides management with a tool not only for innovation, but also for protection against legal claims, as it demonstrates the controllability of the process, proportionality and respect for rights. Thus, a full disclosure of the topic in a practical sense shows that regulatory support for management in a digital environment appears as a system of interconnected policies, procedures, responsibility, control, and a culture of compliance with rules, which simultaneously supports efficiency and guarantees legality.

Table 4 describes governance roles and responsibilities that make legally sound digital transformation possible, and it clarifies decision rights and escalation rules that prevent responsibility gaps. Digital transformation often fails on governance rather than technology, because responsibilities are unclear, decision rights are informal, and escalation is delayed until a crisis forces action. The table therefore treats governance as an operating system for legality and accountability. Oversight bodies set the tone for ethical boundaries and risk appetite, executive management owns outcomes and resource allocation, legal and compliance functions translate

obligations into workable rules, information security leadership ensures control operation and incident readiness, data governance leadership keeps data use tied to purpose and transparency, and process owners ensure day to day conformity. Each role contributes a different type of assurance, and the system becomes reliable only when these contributions are coordinated rather than competing.

Table 4

Governance roles and responsibilities for legally sound digital transformation management

Role or governance body	Core responsibilities in the legal and managerial sense	Decision rights and escalation rules	Expected outputs that demonstrate accountability
1	2	3	4
Board or supervisory level governance	It sets the tone for legality, ethics, and risk appetite in digital transformation and ensures that management resources match the risk profile. It must demand evidence of control and not rely on optimistic narratives about technology	It approves high impact initiatives, requires periodic reporting, and escalates unresolved risks. It can mandate independent reviews when management reports are inconsistent with incident trends or audit findings	Governance principles, approved risk appetite statements, periodic oversight minutes, and decisions on remediation priorities. Records should show active challenge and follow up, not passive acknowledgment
Executive management and business leadership	It owns the transformation outcomes and the legal consequences of operational choices, including how processes, data, and vendors are used. It ensures that legal compliance is built into delivery timelines and budgets	It decides on process redesign, delegations, and acceptance of residual risks with documented justification. It escalates to board level when risks exceed appetite, or when incidents could cause major harm	Signed approvals of major initiatives, allocation of owners and budgets, transformation roadmaps with compliance milestones, and management attestations supported by evidence

(End of Table 4)

1	2	3	4
Legal and compliance function	It translates external obligations into practical rules and ensures contracts, policies, and procedures align with actual operations. It supports incident response and regulatory interactions with consistent documentation and communications discipline	It has veto or escalation rights for initiatives that lack lawful basis, adequate controls, or contract protections. It escalates repeated non compliance patterns to executive management and governance bodies	Policy suite ownership, contract templates, legal review records, compliance registers, audit readiness packs, and documented regulatory communications procedures
Information security leadership	It designs and operates security controls that support confidentiality, integrity, and availability, and it provides evidence that controls work in practice. It also ensures incident response is tested, documented, and legally compatible	It can require security gating before go live, enforce access and configuration standards, and escalate critical vulnerabilities and incidents. It coordinates with legal and business leaders on notification and evidence preservation	Security control catalogs, monitoring reports, vulnerability remediation records, incident response exercise reports, and post incident improvement plans with tracked completion

Source: Formed by the author

Regulatory and legal support for management in the context of the digital transformation of society appears as a system that must work not only within the organization, but also in interaction with the external environment, where regulatory requirements, contractual expectations of partners, market standards and social criteria for the acceptability of management practices operate. At the same time, the digital environment expands the number of points of contact between the organization and stakeholders, as electronic service channels, remote communication formats, platforms for data exchange and service integration make management decisions more

visible, and their consequences faster and more extensive. At the same time, the requirement for consistency is complicated, when internal rules, real settings of information systems and external obligations must coincide, otherwise gaps arise, which often lead to incidents, disputes and loss of trust. Thus, institutional and organizational integration is a condition for ensuring that legal certainty does not collapse under the pressure of the speed of digital change, and that management receives a stable course of action in situations of uncertainty.

Interaction with state authorities in the digital environment requires a transition from formal compliance with requirements to a managerial discipline of preparedness, when the organization has pre-defined procedures for responding to requests, inspections, appeals from subjects of rights, as well as to incidents that may require notifications or cooperation with authorized structures. At the same time, it is important for management to understand which processes create regulatory risk, who is authorized to make decisions on the provision of information, and how confidentiality and integrity of data are ensured during such interaction. At the same time, it is appropriate to form a procedure for internal approval of external communications so that messages are accurate, legitimate and do not create additional claims due to contradictory formulations or incomplete facts. Therefore, this means that legal support becomes an element of reputational and legal resilience management, and not just a post-event response tool.

An important component of integration is the standardization of management procedures, when the organization relies on international approaches to information security management, risk management, change control, business continuity and data management. At the same time, the value of standards lies not in the formal reference to them, but in the transfer of their principles into real processes, in particular, in regular review of access, in documenting authorizations, in configuration control, in testing backup recovery, in maintaining event logs and in the discipline of corrective actions. At the same time, a standardized approach facilitates dialogue with partners and counterparties, as a common language is agreed on the level of control, the responsibilities of the parties and the expected evidence. Thus, the organization receives a tool that simultaneously supports management efficiency and strengthens the legal position in case of disputes, because it is possible to show not only the presence of policies, but also the consistency

of their application. The internal culture of compliance requires separate disclosure, as digital transformation often provokes situations where employees bypass procedures for the sake of speed, and managers tolerate such practices if they give a short-term result. At the same time, a culture of compliance is formed through clear management expectations, consistency of reactions to violations, high-quality training and clear explanations of why the rule exists, what risks it reduces and what the consequences of ignoring it are. At the same time, feedback channels are needed where employees can report process shortcomings or risky situations without fear of unreasonable pressure, and management, for its part, must demonstrate that such reports lead to improvements. Thus, legal enforcement ceases to be an external coercion and becomes an internal managerial norm of behavior that supports the stability of digital processes. At the same time, digital transformation requires a change management system that ensures synchronization between the text of policies, actual processes and information system settings. At the same time, any change, such as launching a new service, integrating with an external platform, switching to remote work formats, automating approvals, or implementing new analytical mechanisms, should undergo an assessment of legal consequences before launch, so that there is no need to urgently correct violations after complaints or incidents appear. At the same time, change management should include document version control, recording decisions, identifying responsible persons, checking the readiness of training materials, as well as confirming that roles, accesses, and event logs are configured in the system in accordance with the agreed procedure. Therefore, this means that management receives a controlled process where the speed of implementing solutions based on applied digital technologies does not destroy legality and does not create hidden risks.

Further areas for improving regulatory management support are related to deepening data management, strengthening control of supply chains of technological services, as well as formalizing the rules for using artificial intelligence-based technologies in decisions that significantly affect people and counterparties. At the same time, special attention needs to be paid to the transparency and explainability of algorithmic recommendations, human control in critical decisions, non-discrimination and the availability of appeal procedures so that digital transformation does not undermine trust and does not create systemic conflicts. At the same time, it is important

to strengthen evidence through high-quality event logs, regular checks of procedure implementation, discipline in closing corrective actions and understandable management reports that reflect not declarations, but the real state of compliance. Thus, the chapter concludes with the position that institutional and organizational integration and a culture of compliance with rules are the conditions that ensure manageability, stability, and legitimacy of management in a digital environment where errors scale quickly and trust is formed slowly.

An effective model of normative and legal support in a digitally transforming organization requires continuous monitoring and disciplined evaluation, because technology, business processes, and regulatory expectations evolve faster than traditional governance cycles. A stable governance system therefore depends on a management approach where compliance is treated as an operational capability, not as a periodic event. Such an approach connects legal requirements with process design, system configuration, and day to day managerial behavior, so that the organization can demonstrate legality and accountability at any moment, including during audits, disputes, or incident investigations. Digital transformation increases visibility of actions through electronic traces, yet it also increases the speed at which errors can propagate, so monitoring must focus on early signals and structural weaknesses rather than on late stage symptoms. A practical governance model places emphasis on traceability, role clarity, and evidence quality, because evidence is what transforms declared compliance into defensible compliance.

A structured evaluation framework begins with defining what “good” looks like in measurable terms for the organization’s internal and external environment. Legal conformity alone is not sufficient if the governance system is too slow to support business delivery, while operational speed alone is not acceptable if legality becomes improvised. A balanced framework therefore assesses whether internal rules are aligned with external obligations, whether system settings enforce those rules, whether responsibilities are clearly assigned, and whether managers can prove that controls operate consistently over time. Key evaluation objects include electronic document validity, integrity of records, correctness of delegation and approvals, access governance, retention and deletion discipline, vendor obligations and performance, and readiness for incident response. A mature

framework also tests whether policies are understandable and usable, because unclear procedures often produce informal workarounds that later create legal exposure. Evaluation should be repeated on a planned cycle and also triggered by major changes, such as new platforms, new data use cases, new outsourcing arrangements, or the adoption of technologies based on artificial intelligence for decision support.

Monitoring needs reliable indicators that connect legal risk with operational reality. Strong indicators are those that reflect control operation, not merely the existence of documents. Examples include frequency of privileged access changes, timeliness of access revocation after role changes, rate of policy exceptions and their closure, completeness of audit logs for critical workflows, percentage of systems covered by retention rules that are technically enforced, results of backup restoration tests, vendor incident notification performance, and the time required to produce legally relevant records on request. Equally important are indicators related to people and workplace governance, such as completion of training tied to specific roles, quality of comprehension checks, frequency of repeated violations, and use of reporting channels for concerns. For algorithm supported decision making, monitoring should include model version control, documented approvals for deployment changes, stability checks, bias testing signals, and volumes of contested outcomes that required human review. Such indicators help management identify where the governance system is weakening, long before a serious breach, regulatory complaint, or contractual dispute forces a reactive response.

A continuous improvement cycle becomes effective only when the organization can convert findings into corrective actions with clear ownership and verifiable completion. Each identified gap should be linked to a specific process owner, a deadline, and an evidence requirement that proves the improvement is real in practice. Corrective actions may involve updating policies, redesigning workflows, tightening role based access, strengthening segregation of duties, improving log retention, refining vendor contracts, or adding stronger review steps for high impact decisions. Digital environments allow improvements to be embedded directly into systems, which reduces reliance on human memory and reduces variability across teams. At the same time, improvement plans must avoid creating unnecessary friction, because overly complex controls encourage bypass

behavior. A well designed improvement process therefore tests whether controls are proportionate to risk, whether they reduce ambiguity for managers, and whether they strengthen defensibility by producing reliable evidence without slowing essential operations.

Independent assurance and internal challenge mechanisms strengthen credibility and reduce blind spots. An organization benefits when internal audit, compliance testing, and information security assurance follow a risk oriented plan that prioritizes the most sensitive processes and the most exposed data flows. Assurance should validate both design and operation of controls, meaning it checks not only whether a rule exists, but whether it is consistently followed, technically enforced where possible, and supported by reliable records. Vendor and outsourcing assurance is especially important, because many digital transformation failures originate outside the organization's direct operational control. Assurance practices should therefore include vendor risk reviews, verification of contractual safeguards in real operations, testing of incident cooperation paths, and confirmation that exit plans are workable. A strong assurance approach also evaluates the human oversight model for technologies based on artificial intelligence, verifying that escalation routes, explainability expectations, and appeal procedures operate as intended, particularly in decisions that can materially affect employees, customers, or partners. Long term sustainability depends on culture, leadership behavior, and governance routines that keep legality aligned with transformation speed. Leadership must reinforce that rule adherence is a performance expectation, not a negotiable preference, and it must do so through consistent decision making and consistent reactions to violations. Training must be role specific and connected to real workflows, so that employees understand what to do, why it matters, and how the organization verifies compliance. Change management must include legal and control evaluation before deployment, so that new tools and new process designs are launched with the necessary safeguards already embedded. Over time, the organization should aim for a governance posture where legality is built into planning, procurement, process design, system configuration, and operational monitoring, creating a stable and defensible trajectory of digital transformation. Such a trajectory strengthens trust, reduces dispute costs, improves resilience, and allows innovation to scale without accumulating hidden legal and operational debt.

Conclusions

Thus, the full disclosure of the topic confirms that the regulatory and legal support of management in the context of the digital transformation of society is not an auxiliary legal formality, but a basic condition for the stability of management in the internal and external environment of the organization. At the same time, digital changes accelerate decision-making, increase dependence on data and automated processes, and therefore, any gap in legal rules often turns into an operational problem, conflict of interest or legal vulnerability. At the same time, it is the conceptual approach that provides the opportunity to move from fragmented reactions to new technologies to the systematic formation of the foundation, where law and management mutually reinforce each other. As a result, the organization receives not only a tool for compliance with requirements, but also a prerequisite for trust, predictability and manageability of digital transformations. This means that theoretical and methodological foundations are key to aligning management functions with legal principles, including legality, certainty, proportionality, accountability, data protection and fairness. At the same time, these principles must be translated into a clear management language of processes, powers, control points and responsibilities, otherwise they remain declarations. At the same time, the multi-level nature of legal regulation, from general guarantees of human rights to internal policies, emphasizes that the effectiveness of legal support depends on the consistency of norms and practices, not on their quantity. Thus, the focus is on the ability of an organization to integrate legal requirements into the design of digital processes, ensuring the evidence of management actions and the reproducibility of decisions in the event of disputes and audits. At the same time, the practical aspect of the topic demonstrates that the real effectiveness of regulatory and legal support is manifested through internal policies, procedures and regulations that detail the requirements of the law for specific business processes. At the same time, it is precisely the integration of these rules into everyday management activities that provides an opportunity to reduce legal risks without losing the speed and flexibility that digital transformation requires. Often, key tools become process responsibility, separation of powers, logging of actions, access control, contractual requirements for contractors, as well as control and audit as mechanisms for maintaining compliance. Thus, law appears

as a practical tool for managing resilience, and not only as a response to violations after the consequences have already occurred.

At the same time, the digital environment enhances the importance of cybersecurity and incident response, where the legal correctness of procedures becomes as important as technical efficiency. At the same time, incidents require predetermined decision-making procedures, preservation of evidence, communication with customers and partners, as well as interaction with state authorities in cases provided for by law. It is not uncommon for it to be proper documentation, clarity of roles and verifiability of actions taken that provide an organization with the opportunity to substantiate good faith and reduce the scale of legal consequences. At the same time, the role of internal training and the formation of a culture of compliance with the rules increases, since even the best technological means do not compensate for the human factor when employees do not understand the requirements or ignore them in their daily work. Thus, this leads to the conclusion that the regulatory and legal support of management in the conditions of digital transformation of society must develop as a holistic system, where principles, procedures, control, responsibility and ethical guidelines are combined, including the rules for the use of technologies based on artificial intelligence. At the same time, the algorithmization of decisions increases the requirements for transparency, non-discrimination, explainability and human control, as well as the possibility of appealing and reviewing decisions in case of errors. At the same time, the long-term effect of such a system is that the organization gains not only compliance with the requirements, but also competitive advantages, because legal certainty simplifies scaling, reduces transaction losses, increases the trust of partners and maintains stability in periods of rapid technological change. Therefore, this means that it is the conceptual principles and their practical implementation that form the basis for effective management in a digital environment, which is simultaneously effective, safe and legitimate.

References:

1. Lorenz, L., van Erp, J., Meijer, A. (2022). Machine-learning algorithms in regulatory practice: Nine organisational challenges for regulatory agencies. Technology and Regulation, pp. 1-11

2. Ulbricht, L., Yeung, K. (2022). Algorithmic regulation: A maturing concept for investigating regulation of and through algorithms. *Regulation & Governance*, Vol. 16, No. 1, pp. 3-22

3. Gritsenko, D., Wood, M. (2022). Algorithmic governance: A modes of governance approach. *Regulation & Governance*, Vol. 16, No. 1, pp. 45-62

4. Coglianese, C., Lehr, D. (2019). Transparency and Algorithmic Governance. *Administrative Law Review*, Vol. 71, No. 1, pp. 1-56

5. Heimburg, V., Wiesche, M. (2023). Digital platform regulation: opportunities for information systems research. *Internet Research*, Vol. 33, No. 7, pp. 72-85

6. Schneider, J.-P., Erny, J., Enderlein, F. (2025). Collaborative Governance Structures for Interoperability in the EU's new data acts. *European Journal of Risk Regulation*, Vol. 16, No. 1, pp. 24-35

7. Veale, M., Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International,* Vol. 22, No. 4, pp. 97-112

8. Andrews, L. (2019). Public administration, public leadership and the construction of public value in the age of the algorithm and 'big data'. *Public Administration*, Vol. 97, No. 2, pp. 296-310

9. Alazzam, F.A.F., Shakhatreh, H.J.M., Gharaibeh, Z.I.Y., Didiuk, I., Sylkin, O. (2023). Developing an information model for E-Commerce platforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance. *Ingénierie des Systèmes d'Information*, Vol. 28, No. 4, pp. 969-974

10. Zybareva, O., Shylepnytskyi, P., Ozarko, K., Kravchuk, I., Nahorniuk, O. (2023). The organizational and economic mechanism of attraction of digital technologies in the innovation activity of companies in the conditions of international competition. *Revista de la Universidad del Zulia*. Vol. 14, No. 39. pp. 415-431.