Viktorija Adamić Ciglar
univ.mag.ing.traff
Logistics and Sustainable mobility,
University North,
Koprivnica,
Croatia
viadamic@unin.hr

Article info:
Submitted: June 13, 2024
Accepted: September 15, 2024
UDC: 65.011.3
DOI: 10.38190/ope.14.2.1

ORIGINAL SCIENTIFIC PAPER

ISSN 1849-7845
ISSN 1849-661X

LEGAL RISKS AND THEIR MANAGEMENT ACCORDING TO STANDARD 31022:2022

Abstract: *Managing legal risks is becoming an increasingly significant part of corporate governance, especially in the context of increasingly complex legislative frameworks and growing compliance requirements.*

The ISO 31022:2022 standard provides guidelines for effective legal risk management, complementing the broader frameworks of ISO 31000:2014 and ISO 31010:2019. This article explores the principles, processes, and tools for managing legal risks and emphasizes the importance of integrating them into overall business strategies.

Legal risks, defined as the possibility of negative consequences arising from legal issues, include contractual risks, compliance risks, regulatory risks, and intellectual property. Managing these risks requires an effectively structured approach. The use of tools such as analytics, simulations, and legal databases enables better decision-making and the mitigation of potential damages.

The article also highlights the role of education and communication in building an organizational culture focused on legal risk management. It is important to note that implementing legal risk management contributes to business stability, strengthens stakeholder trust, and enables organizations to be more resilient to legal challenges.

Keywords: *legal risks; ISO 31022; risk management; compliance; corporate governance*

1. Introduction

Legal risks are present in almost every aspect of business operations. They often arise from non-compliance with laws, failure to meet contractual obligations, violations of intellectual property rights, and numerous other situations that can have serious consequences for an organization. Modern businesses face challenges from an increasingly dynamic legislative environment, growing compliance demands, and global changes in business practices. These factors lead to bureaucratic bottlenecks and, consequently, significant risks. *(Croatian Standards Institute. (2022). „Risk management -Guidelines for legal risk management (ISO 31022:2022)". Croatian Standard HRN ISO 31022:2022.)*

Legal risks are generally defined as potential events that can result in financial losses, legal proceedings, or reputational damage to an organization. Their importance lies in their impact on the operational stability and long-term sustainability of the organization.

The ISO 31000:2014 and ISO 31010:2019 standards establish guidelines for the identification, analysis, and management of risks, while ISO 31022:2022 extends the focus to specific legal risks. These standards not only provide tools but also encourage organizations to integrate legal risk management into their overall strategies.

2. Legal risks and their classification

Legal risks pertain to potential negative consequences arising from legal obligations, regulatory non-compliance, or failure to fulfill contractual terms. These risks can lead to financial losses (e.g., legal penalties, attorney fees, or lost contracts), reputational damage (e.g., long-term loss of stakeholder trust), and operational consequences (e.g., business interruptions due to legal disputes). *(Croatian Standards Institute. (2022). „Risk management - Guidelines for legal risk management (ISO 31022:2022)". Croatian Standard HRN ISO 31022:2022.)*

Legal risks can be categorized into five *(5)* main groups:

1. Contractual Risks

These risks arise from the failure to adhere to contractual terms or from entering into agreements with unfair conditions or ambiguous clauses.

Example: A company failing to fulfill its obliga-

tions for product delivery under a contract may face penalty claims for damages.

2. Compliance Risks

Compliance risks are associated with non-adherence to laws such as GDPR or labor regulations. Non-compliance can result in severe fines and a loss of trust among employees and/or clients.

Example: A company failing to ensure GDPR compliance may face penalties of up to 4% of its global annual turnover.

3. Regulatory Risks

These risks occur when laws or regulations change drastically or frequently, impacting business models.

Example: A change in tax legislation may require significant adjustments in financial reporting processes.

4. Intellectual Property Risks

Intellectual property risks involve violations of copyrights, patents, or trademarks.

Example: An organization using a protected design without permission may face lawsuits for infringement.

5. Third-Party Liability Risks

These risks encompass lawsuits filed by customers, employees, or suppliers.

Example: Claims due to workplace injuries or lawsuits for defective products.

Based on these categories, legal risks can be hierarchically organized into three overarching categories to illustrate the relationship between risks and their consequences for business operations. *(Croatian Standards Institute (2019). „Risk management - Risk assessment methods (ISO 31010:2019)". Croatian Standard HRN EN IEC 31010.*

Focusing on specific risks, such as poorly structured contracts or failure to meet regulatory deadlines, lays the foundation for establishing essential risk management measures. Such visual representation helps in identifying key areas requiring action within the organization to ensure legal compliance and safeguard the organization's reputation.

3. Management and monitoring of legal risks

3.1. Management

The ISO 31000 and ISO 31022 standards propose eight (8) key principles for effective legal risk management:

1. Integration

Legal risk management must be an integral part of overall business operations.

Example: Considering legal risks when making strategic decisions.

2. Structured and Comprehensive Approach

A consistent approach that takes into account all aspects of the legal environment.

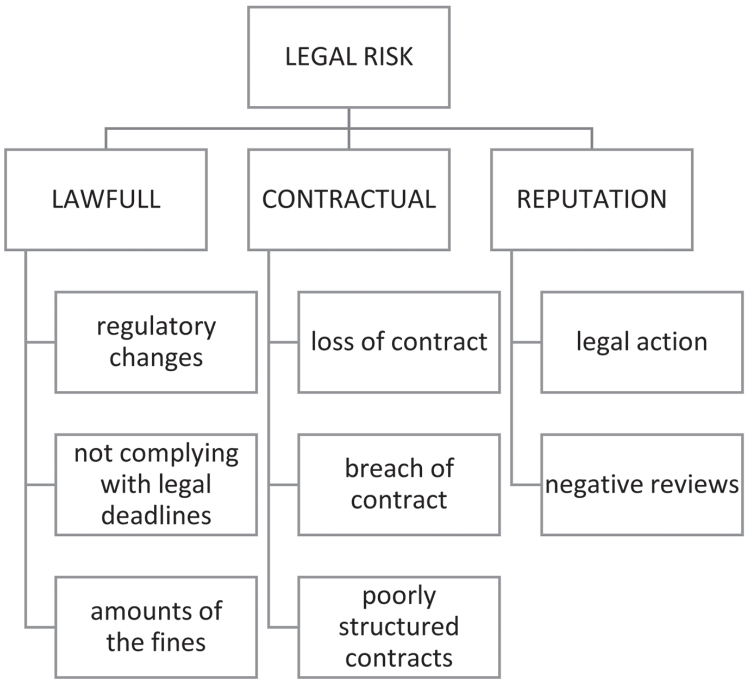

Figure 1. Risk Hierarchy (Source: Author's Work)

Example: Using legal databases to analyze potential implications of new regulations.

3. Adaptability

The approach must align with the specific needs of the organization.

Example: Smaller companies may engage external consultants to reduce costs.

4. Inclusivity

Active involvement of all stakeholders.

Example: Employees are educated about their legal responsibilities within the organization.

5. Dynamism

Adapting to changes in the legislative environment.

Example: Regular monitoring of new environmental protection laws.

6. Best Available Information

Using relevant data to make informed decisions.

Example: Scenario simulations to assess potential consequences of contracts.

7. Human and Cultural Factors

Considering different perspectives and perceptions of risks.

Example: Multinational organizations account for the legal norms of different countries.

8. Continuous Improvement

Learning from past experiences and adopting new strategies.

Example: After a court ruling, the organization updates its internal policies.

Legal risk management processes are thoroughly described through the phases of *identification, analysis, evaluation, and treatment. (Croatian Standards Institute. (2019). „Risk management - Risk assessment methods (ISO 31010:2019)". Croatian Standard HRN EN IEC 31010.)*

Identification of Legal Risks

- Tools for identification: Legal audits, questionnaires, workshops.
- Example of practice: An organization develops a legal risk register encompassing contractual, regulatory, and operational risks.

Analysis of Legal Risks

- Qualitative and quantitative analysis: Assessment of probability and consequences.
- Analysis techniques: SWOT analysis, analytical tools, and artificial intelligence.
- Example: A bank analyzes the implications of changes in anti-money laundering laws.

Evaluation of Legal Risks

- Description: Comparing risks against the organization's established criteria.
- Example: The organization ranks legal risks based on their impact on reputation.

Treatment of Legal Risks

- Description: Includes developing treatment plans and proactive measures such as employee education and improvement of internal organizational policies.
- Strategies: Avoidance, reduction, transfer, or acceptance of risks.
- Example: A company uses insurance to cover potential lawsuits.

When managing risks within an organization, it is essential to consider both the external and internal environment of the risks being addressed, as well as the guidelines provided by ISO 31000:2018. Legal risks represent specific and highly critical risks, requiring separate analysis of their environments.

The **external environment** of legal risks includes factors outside the organization:

- Laws and their changes (both local and international),
- External stakeholders (regulatory bodies, media, interest groups),
- Third parties (e.g., service providers, law firms),
- External influences (agreements, market conditions, jurisdictional conflicts).

When analyzing the **external environment**, it is crucial to account for differences in laws, cultures, and environmental conditions, as well as the mutual recognition of laws when dealing with regulations from other countries.

The **internal environment** of legal risks encompasses factors under the organization's control, such as:

- Legal entities and business model,
- Internal legal structure and governance systems,
- History of legal disputes and current legal situation,
- Organizational assets (both tangible and intellectual),
- Policies, processes, and resources for managing legal risks.

Organizations should develop and adapt their legal risk criteria based on actual situations. Legal risk criteria are the standards or benchmarks an

Figure 2. External Environment of legal risks (Source: Author's Work)

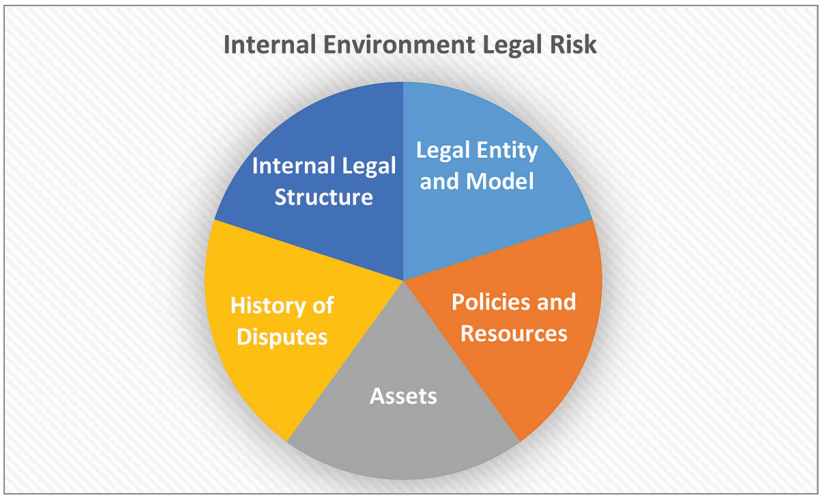

Figure 3.Internal Environment of legal risks (Source: Author's Work

organization uses to assess, analyze, and manage legal risks. They define how the organization will identify, evaluate, and decide whether to accept, mitigate, transfer, or avoid legal risks. *(Croatian Standards Institute. (2018). Risk management - Guidelines (ISO 31000:2018). Croatian Standard HRN ISO 31000.)*

Effective legal risk criteria must:

- Reflect the organization's objectives and risk tolerance,
- Be dynamic and aligned with the overall risk management approach,
- Include factors such as organizational priorities, relationships with third parties, and legal risk categorization.

Overly restrictive criteria for legal risks that are not in alignment with the general risk criteria of the organization can result in a poor approach to legal risk management. This often leads to the involvement of legal experts only in crisis situations, instead of during the early stages when their timely input could significantly reduce risks and ensure more efficient management

3.2. Monitoring Legal Risks

Legal risk management involves regular monitoring of legislative changes, enabling organizations to identify potential threats and adapt their business processes to meet new requirements, thereby reducing the risk of sanctions, lawsuits, and reputational damage. *(Croatian Standards Institute. (2022). „Risk management - Guidelines for legal risk management (ISO 31022:2022)". Croatian Standard HRN ISO 31022:2022.)*

Organizations must implement systems for tracking legislation to stay updated on regulations that impact their operations. This includes monitoring local, national, and international laws that may affect specific sectors.

Monitoring legal risks also requires continuous education and raising employee awareness about

relevant legal regulations to minimize the risk of unintentional violations. Collaboration with legal experts or the use of specialized software (e.g., Hyperproof[1]) for automated tracking of legal changes enhances the efficiency of risk management. Analyzing the impact of legislative changes on existing contractual obligations and operational processes is crucial to avoiding situations of non-compliance or failure to fulfill contractual duties.

The best example of this is organizations operating within the European Union, which must monitor changes in GDPR regulations (General Data Protection Regulation). Regular adjustments to privacy policies and personal data management enable them to avoid hefty fines, which can reach up to 4% of the company's global annual turnover. Moreover, compliance with GDPR contributes to maintaining the trust of clients and business partners.

3.3. Key Risk Indicators (KRI)

Key risk indicators allow organizations to quantify and monitor potential legal issues. Measuring these indicators ensures a timely response to risks and contributes to reducing legal costs. *(Croatian Standards Institute. (2018). „Risk management - Guidelines (ISO 31000:2018)". Croatian Standard HRN ISO 31000.)*

One key risk indicator can be the ratio of lawsuits to the number of contracts. This indicator reflects the frequency of legal disputes relative to the total number of contracts the organization has entered into. A high ratio may signal deficiencies in contract terms, inadequate legal oversight, or poor relationships with clients and partners. Regular analysis of this ratio enables the legal team to identify the causes of disputes and adjust contract terms to reduce the likelihood of conflicts. Another essential key risk indicator for legal risks is the analysis of legal dispute costs over a specific period.This indicator examines the total costs associated with legal processes, including attorney fees, penalties, compensation, and administrative expenses. An increase in costs may indicate systemic issues that need to be addressed. For instance, if a company notices a rise in legal dispute costs over the past year, it can initiate internal investigations to determine the causes—such as non-compliance with regulations, poorly defined contractual obligations, or inadequate employee training.

Monitoring legal risks is not just a legal obligation but also a strategic advantage that ensures business continuity and reduces expenses. By utilizing KPIs and promptly monitoring legal changes, organizations can effectively manage legal risks, avoid unnecessary losses, and strengthen their position in the market.

3.4. Practical Examples Illustrating management of Risks

Successful Management of Legal Risks

- **Pfizer Inc.**[2]

  Pfizer Inc., a major pharmaceutical company, successfully implemented a system for monitoring regulatory changes. As part of this system, the company engaged specialized legal advisors and utilized software solutions for automated tracking of new laws.

  Outcome: When stricter regulations on drug labeling were introduced, the company promptly adjusted its products and documentation. This proactive approach helped Pfizer avoid fines amounting to millions of dollars and retain its licenses to sell in key markets.

- **Microsoft**

  In 2018, Microsoft introduced stringent internal policies and procedures to ensure compliance with the General Data Protection Regulation (GDPR) of the European Union. The company conducted extensive employee training, adjusted its products and services, and established transparent data processing practices.

  Outcome: This approach allowed Microsoft to avoid significant fines and maintain user trust.

  (https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data)

- **Apple**

  Over recent years, Apple has taken steps to mitigate legal risks related to user privacy. One example is the introduction of the App Tracking Transparency (ATT) feature, giving users greater control over the data collected by apps.

  Outcome: This initiative helped Apple avoid regulatory penalties in jurisdictions with high privacy standards, such as the EU, and strengthened the company's brand as a protector of user privacy.

  (https://developer.apple.com/documentation/apptrackingtransparency)

[1] https://hashdork.com

[2] https://www.pfizer.com

- **Kones – Bi d.o.o. (Croatia)**

  Kones – Bi d.o.o., a Croatian producer of table eggs, withdrew certain batches from the market due to the presence of Salmonella Typhimurium on its farm. This preventive recall included class A eggs, grade "M," from floor-reared hens, with an expiration date of December 1, 2024. The product did not comply with the Regulation on General Food Law and safety standards set by the European Food Safety Authority.

  Outcome: The company conducted a thorough analysis of its products and ensured compliance with new EU food labeling regulations. Timely adjustments helped avoid potential penalties and product recalls, preserving the company's reputation and consumer trust.

  (https://www.hapih.hr/opoziv-proizvoda-konzumna-jaja-kones-bi-d-o-o-2/)

Unsuccessful Management of Legal Risks

- **Facebook (Meta Platforms Inc.)**

  A technology company in the software development sector, Facebook (Meta Platforms Inc.), failed to update its contractual clauses in line with changes in intellectual property laws.

  Consequences: One of its key partners filed a lawsuit over copyright infringement. The result was the loss of a contract and the payment of compensation amounting to several million dollars, along with additional legal costs and reputational damage in the mark.

  (https://www.reuters.com/legal/litigation/authors-can-depose-meta-ceo-zuckerberg-ai-copyright-case-judge-says-2024-09-25)

- **British Airways**

  In 2018, British Airways suffered a major security breach compromising the persona data of hundreds of thousands of users. An investigation revealed that the company had not adequately implemented the security measures required under GDPR.

  Consequences: The UK Information Commissioner's Office (ICO) imposed a fine of £20 million on British Airways, which was the largest GDPR-related fine at the time.

  (https://www.bbc.com/news/technology-54568784)

- **Volkswagen Dieselgate Scandal (2015)**

  Volkswagen manipulated emissions tests using software, violating environmental laws in the US and EU.

  Consequences: The company faced penalties exceeding $30 billion and suffered a significant loss of customer trust and reputation. *(https://www.bbc.com/news/business-34324772)*

- **Konstruktor-Inženjering (Split, Croatia)**

  The construction company "Konstruktor-Inženjering" from Split faced financial problems and legal disputes due to failure to fulfill contractual obligations on projects in Croatia and abroad (e.g., highway construction).

  Consequences: The company did not timely adapt its contracts with subcontractors to comply with new labor law provisions. As a result, it faced lawsuits from workers over labor rights violations, leading to substantial financial losses and damage to the company's reputation.

  (https://www.vecernji.hr/biznis)

4. Conclusion

The integration of legal risk management into business strategies is essential for ensuring the stability and sustainability of an organization. The ISO 31000:2014 and ISO 31022:2022 standards provide a valuable framework for structured and effective risk management. Through the identification, analysis, and treatment of legal risks, organizations can significantly reduce potential losses and enhance compliance with legislative requirements.

In addition to meeting legal obligations, effective legal risk management improves operational efficiency by minimizing disruptions caused by legal disputes or non-compliance. Transparent processes, clearly defined roles and responsibilities, and the continuous improvement of internal policies create a strong foundation for long-term success. Organizations that invest in employee education and the implementation of advanced tools for tracking legislation foster a culture of readiness and accountability. This readiness enables adaptation to challenges in the legal and regulatory environment, ensuring compliance and a competitive edge in the market.

In conclusion, effective legal risk management enables organizations to become more resilient to external and internal challenges. Transparent processes, clearly defined responsibilities, and continuous improvement are key to long-term success.

References

Croatian Standards Institute. (2018). Risk management - Guidelines (ISO 31000:2018). Croatian Standard HRN ISO 31000.

Croatian Standards Institute. (2019). Risk management - Risk assessment methods (ISO 31010:2019). Croatian Standard HRN EN IEC 31010.

Croatian Standards Institute. (2022). Risk management - Guidelines for legal risk management (ISO 31022:2022). Croatian Standard HRN ISO 31022:2022.

Smjerog, S. (2017). Standards and standardization. Specialist professional thesis, Polytechnic of Karlovac. Retrieved August 4, 2024, from https://urn.nsk.hr/urn:nbn:hr:128:195307.

Ćatić, I., & Arsovski, S. (2011). FMEA in product development phase. In 5th International Quality Conference, Kragujevac.

Čičak, I. (2017). Risk assessment methods. Retrieved from https://urn.nsk.hr/urn:nbn:hr:235:788376.

Kassimi, A. (2023). Integration of different Risk Assessment methods and techniques to achieve effective Risk Management in the context of Process Safety. Retrieved from˝https://apothesis.eap.gr/archive/item/188589.

Adamić Ciglar, V. (2024). Systematic review of risk assessment methods and techniques using ISO 31010:2019 (Master's Thesis). Koprivnica: University North. Retrieved from https://urn.nsk.hr/urn:nbn:hr:122:577756

Pfizer. (2014 – 2023). (Pfizer company information). Retrieved from https://www.pfizer.com

Facebook. (2021, October). Facebook company is now Meta. Retrieved from https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

Lider Media. (2023, August 9). A powerful tool for small businesses: A guide to strategic business risk management. Retrieved from https://lidermedia.hr/sto-i-kako/mocni-alat-malih-poduzeca-vodic-za-stratesko-upravljanje-poslovnim-rizicima-152409

Hashdork. (2024.). (Hashdork company information). Retrieved from https://hashdork.com

World of Quality (2019, July 4.). New edition of IEC 31010:2019. Retrieved from https://www.svijet-kvalitete.com/index.php/normizacija/4424-novo-izdanje-iec-31010-2019

ISO. (2024). (ISO website). Retrieved from https://www.iso.org

UpGuard. (2024, October). Third-party risk management. Retrieved from https://www.upguard.com/category/third-party-risk-management

Micrtosoft. (2018, May 21). Microsofts commitment to GDPR privacy and putting customers in control of their own dana. Retrieved from https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data.

Večenji list. (2012, July 20). Konstruktor's account has been unfrozen, and roadworks are continuing. Retrieved from https://www.vecernji.hr/biznis/konstruktoru-deblokiran-racun-nastavljaju-se-radovi-na-cestama-444569.

BBC News. (2015, September 22). Volkswagen: The scandal explained. Retrieved from https://www.bbc.com/news/business-34324772.

BBC News. (2020, October 15). Apple faces EU privacy investigations over Siri recordings. Retrieved from https://www.bbc.com/news/technology-54568784.

Hals, T. (2024, September 15). Authors can depose meta CEO Zuckerberg in AI copyright case, judge says. Retrieved from https://www.reuters.com/legal/litigation/authors-can-depose-meta-ceo-zuckerberg-ai-copyright-case-judge-says-2024-09-25.

Croatian Agency for Agriculture and Food, (2024, November 8.). Product recall cunsumer eggs Kones BI d.o.o. Retrieved from https://www.hapih.hr/opoziv-proizvoda-konzumna-jaja-kones-bi-d-o-o-2/

Apple Inc. (2022, April 26). Mobile Advertising and the Impact of Apple's App Tracking Transparency Policy. Retrieved from https://developer.apple.com/documentation/apptrackingtransparency