Journal of Applied Economic Sciences
Volume XIX, Summer, Issue 2(84)

Designing Innovative Quick Response Codes-Based Product Authenticity Safeguards: Risk Analysis

Karolina KULIGOWSKA
https://orcid.org/0000-0001-8956-4723
Faculty of Economic Sciences, University of Warsaw, Poland
kkuligowska@wne.uw.edu.pl

Aron HUĆ
ETICOD sp. z o.o., Katowice, Poland
aron@eticod.pl

Article's history:

Received 15th of April, 2024; *Received in revised form* 9th of May, 2024; *Accepted* 12th of June, 2024; *Available online*: 15th of June, 2024. *Published* as article in the Volume XIX, Summer, Issue 2(84), 2024.

Suggested citation:

Kuligowska, K., & Huć, A. (2024). Designing innovative quick response codes-based product authenticity safeguards: Risk analysis. *Journal of Applied Economic Sciences*, Volume XIX, Summer, 2(84), 201 – 207. https://doi.org/10.57017/jaes.v19.2(84).07

Abstract:

This paper examines the potential risks that may occur when designing and implementing innovative products' authenticity safeguards based on quick response (QR) codes. The study identified ten key risks, which were then analyzed in two dimensions: the probability of their occurrence and the strength of their impact, should they occur. Using the matrix-based method, risks were visualized on an intensity scale in both dimensions and with adequate color notation. Subsequently, the identified risks were grouped thematically. This enabled the identification of four key areas containing the identified risks, namely: competition, external websites, technological integration and risks dependent on internal factors. After aggregating individual risk levels, for each key area the average risk level was calculated. The first three areas were characterized by an average low level of risk, while the area related to risks dependent on internal factors was characterized by an average medium level of risk. The study's systematic approach to identify and evaluate risks related to the execution of QR code-based authenticity safeguards project can be applied by businesses to similar projects, as it enables scientific-based risk identification and management, and consideration of strategies to mitigate the potential issues, ensuring smoother project execution and more reliable product performance.

Keywords: product authenticity safeguards, risk analysis, QR codes, anti-counterfeit.

JEL Classification: D81, M21, O32.

Introduction

Counterfeiting products poses a serious threat to many market sectors, although it equally significantly affects public safety and the economy as a whole. In response to this challenge, further safeguards for product authenticity have been developed, such as holograms, barcodes and Radio Frequency Identification (RFID) systems (Bansal et al., 2013). Despite these actions, counterfeiters are using increasingly advanced methods that allow them to bypass traditional security measures.

Designing innovative security measures based on QR codes is a current and important issue (Karrach et al., 2020). The QR code is characterized by a large information capacity - approximately 100 times greater than barcodes - and is also able to support the encoding of logographic and phonemic characters (Petrova et al., 2016); it is more accurate than holograms, highly error-resistant (Li et al., 2017), and at the same time it is easy to use by any user. There is a growing popularity and widespread use of this technology in various areas of life, including: retail, medicine and pharmaceuticals, marketing, automotive and transportation, Internet of Things (IoT) and public services (Huo et al., 2021; Nasr et al., 2023; Aulia et al., 2024).

However, designing a unique innovation of such security is a non-trivial task. Firstly, the end user needs a special application to scan the QR code printed on the product. Secondly, the QR code decoder is not integrated with the application for local decoding due to security risks. To avoid threats, the application captures the image only with the location where it was scanned and sends it to the server.

Finally, a server is needed to decode the image, verify it, and send feedback (Li et al., 2017; Huo et al., 2021). As can be seen from this short description of how a QR code works, designing a QR code-based solution involves not only carrying out an internal technological project by the company, but also its further integration with various external systems. This creates the need to analyze the process of designing and implementing the solution in terms of risks, threats and potential weaknesses at each stage of its innovative development, which, however, is not a common area of scientific research.

This paper tries to fill this gap and aims to identify the key risks that apply to the design of innovative security measures based on QR codes. This research allows the development of appropriate strategies to minimize the risk of project's failure or security breaches. Thanks to a systematic research approach, the chances of success of innovative technological solutions can be increased.

This paper is organized as follows. Section regarding related work presents an overview of the scientific backgrounds in the context of the development of QR code technology for various industries and the risk analysis related to innovative projects. Section regarding approach describes briefly matrix risk assessment methods on which we focused as our starting point for risk identification, measurement and assessment. Section regarding research results reveals our findings and discusses adequate preventive and corrective actions. Conclusions are included in the last section.

1. Related Work

Scientific research examines the use of QR codes in many different fields. Most often, researchers focus on improving code reading in terms of image processing accuracy (Huo et al., 2021), detecting QR code forgeries and designing anti-counterfeiting security measures (Picard et al., 2021; Wang et al., 2023), integrating solutions based on artificial intelligence, machine learning and natural language processing to strengthen resistance to attack threats (e.g. phishing, quishing, QRLjacking) of QR code technology (Pawar et al., 2022; Vaithilingam and Shankar, 2024), as well as analyzing the advantages and restrictions on the use of QR codes (Petrova et al., 2016).

Many factors, such as the pace of technological progress, keen competition and dynamic changes in the business environment, often make it difficult to adequately assess the effectiveness of planned investments in QR code-based solutions. Therefore, the implementation of innovative projects in the field of QR code technology development requires comprehensive consideration of potential risks and consideration of possible preventive actions that can be taken.

The risk evaluation process is based on risk management. The management of specific risks in an enterprise that arise during the implementation of technologically innovative projects consists of processes related to the identification of threats, their analysis (measurement and assessment of risks), and then the implementation of possible preventive actions and continuous monitoring of the risk level (Deptuła and Knosala, 2015). The first two processes, i.e. risk identification and its analysis, constitute an empirical risk analysis based on the knowledge and experience of risk assessors. If the risk analysis concerns innovative projects, the importance of this task increases, but at the same time it's complicated and difficult to carry out, because there are no universal, clear and specific criteria in this regard (Walas-Trębacz & Bartusik, 2023; Deptuła, 2024). There are many recognized risk assessment methods in the scientific literature. One group of approaches include matrix methods of risk assessment (Murray et al., 2011). The characteristic features of this group of methods are the following (Kovačević et al., 2019):

- they are developed as the first in the risk assessment process,
- they constitute a starting point for other risk assessment methods,
- in practice, they turned out to be most susceptible to the area-specific expertise of all participants in the risk assessment process.

This paper focuses on the risk assessment matrix approach due to its above-mentioned key features, wide presence in scientific literature and high importance in business practice.

2. Research Approach

According to Aven (2016), risk assessment and risk management are scientific fields that make an important contribution to supporting decision-making in business practice. In addition, matrix methods of risk assessment are widely recognized as the starting point for risk measurement and assessment (Murray et al., 2011; Deptuła & Knosala, 2015). The overall advantage of these methods is their relative simplicity and transparency. This allows for adopting various perspectives and risk factors, especially since - according to Berglund (2007) and Gorokhovatskyi et al. (2021) - risk is more closely related to innovation, which involves striving for emerging opportunities in conditions of uncertainty, hence the uniqueness of each innovation and the lack of commonly used, universal methods for objective assessment of an innovative project should be taken into account.

Thanks to these aspects, the risk assessment matrix utilized in this paper is not only a solid analysis tool, but also an appropriate and up-to-date approach to risk management in innovative projects, such as the development of QR code-based technologies and their innovative application possibilities.

3. Research Results

The results of our research reveal risks that may arise in the course of conceptual, executive, and implementation phases of the project. We have identified potential risks, the probability of their occurrence and the impact should they occur, all of which should be taken into account when designing innovative product authenticity safeguards based on QR codes. A total of ten risks with potential impact on the project have been identified and numbered:

1. Online services that generate truly random numbers will be disabled during the project.
2. Inability to implement the project results due to a dispute over intellectual property.
3. The emergence of new technological solutions.
4. The training and test sets created will not sufficiently describe reality.
5. The quality of the code print will be low and therefore illegible.
6. Internet services will be too slow.
7. Mobile devices will not be able to read QR codes.
8. Not all popular web browsers will work with the web application.
9. Not all mobile devices will work with the application.
10. Server failure and/or network failure.

Subsequently, for each identified risk, the calculated risk level was determined according to three ranges in a three-level scale (low, medium, high). The most frequently used form of general risk assessment is its visualization as a matrix marked with colors reflecting the risk's severity (as green, yellow, red). It is also called a risk map and presents risk in two dimensions: probability and impact if it occurs (Murray et al., 2011).

In this paper, each of the risks in both dimensions was given values in the following categories: low, medium, high, expressed numerically as: 0,3 – low; 0,6 – medium; 0,9 – high (Kovačević et al., 2019). Then, the product of the values of both dimensions indicated the risk level in three arbitrarily determined ranges, which included the following values: low (0-0,26), medium (0,27-0,53), high (0,54-0,81). The results are illustrated in the following Table 1.

Table 1. List of identified risks with the calculated risk level

	Risk	Probability	Impact	Risk score	Risk level
1.	Online services that generate truly random numbers will be disabled during the project	0,3	0,3	0,09	Low
2.	Inability to implement the project results due to a dispute over intellectual property	0,3	0,6	0,18	Low
3.	The emergence of new technological solutions	0,6	0,6	0,36	Medium
4.	The training and test sets created will not sufficiently describe reality	0,3	0,6	0,18	Low
5.	The quality of the code print will be low and therefore illegible	0,3	0,3	0,09	Low
6.	Internet services will be too slow	0,6	0,3	0,18	Low
7.	Mobile devices will not be able to read QR codes	0,3	0,3	0,09	Low
8.	Not all popular web browsers will work with the web application	0,3	0,3	0,09	Low
9.	Not all mobile devices will work with the application	0,9	0,3	0,27	Medium
10.	Server failure and/or network failure	0,6	0,9	0,54	High

Source: own elaboration.

Each of the ten risks was then plotted on a risk matrix specifying the probability on one axis and the impact on the other, as shown in the following Table 2.

Table 2. List of identified risks with the calculated risk level

Impact		Probability: Low	Probability: Medium	Probability: High
Impact	High	0	1	0
	Medium	2	1	0
	Low	4	1	1
		Low	Medium	High
		Probability		

Source: own elaboration.

The prepared risk matrix shows that one of the risks is placed in the red zone. Two risks are in the yellow zone and seven are in the green zone. In terms of probability of occurrence, most of them are low-probability risks (6 in total), then medium-probability risks (3 in total), and the fewest are high-probability risks (one). In terms of consequences, most risks (6 in total) are associated with a low level of impact, followed by three risks with a medium level of impact, and finally one risk with high impact.

Most of the identified risks have a low level of both probability of occurrence and potential impact, which is a favorable indicator for the stability and safety of the project. However, special attention should be paid to the risk with a higher threat level (risk no. 10 "Server failure and/or network failure"), and the implemented preventive and corrective measures to minimize this risk should be continuously monitored.

All ten risks were subsequently grouped thematically into four key areas of occurrence. Additionally, the average risk level was calculated for each area:

1. Competition (risk no. 2, risk no. 3). Average risk level: low.
2. External websites (risk no. 1, risk no. 6). Average risk level: low.
3. Technological integration (risk no. 7, risk no. 8, risk no. 9). Average risk level: low.
4. Risks dependent on internal factors (risk no. 4, risk no. 5, risk no. 10). Average risk level: medium.

In order to minimize risk and maximize project success, through a thorough risk analysis and by adapting the project to the changing business and technological environment, preventive actions should then be considered for each risk in each of these areas. As it can be seen, Competition and External websites, along with Technological integration, are areas with low average risks. However, Risks dependent on internal factors area shows a medium average risk level, indicating a need for closer monitoring. Proposed preventive and corrective actions in relation to ten identified risks are presented below, divided and summarized into four key areas.

Competition

In order to minimize the risk and its consequences, it is recommended to conduct a detailed patent analysis to secure intellectual rights and prevent intellectual property disputes. Monitoring market trends will allow to adapt the design strategy to changing market conditions. An important step will also constitute a systematic verification and evaluation of solutions introduced by the competition and improvement of the project in relation to possible activities of the competitors. The involvement of experts in the project will ensure flexible adaptation of the design direction to available technological innovations in the market and maintain the project in line with the latest market expectations. Additionally, in order to faster commercialize the project results, additional expenditure can be used, to accelerate its full execution.

External websites

Recommended actions to minimize risk and ensure business continuity in a changing and sometimes unreliable internet environment include planning the selection of two (or more) websites as a backup strategy. The selection of services that generate truly random numbers should prioritize those that are less prone to failures. Additionally, a key aspect is the use of an algorithm based on a pseudorandom number generator that meets the highest safety and reliability standards, which minimizes the risk of unforeseen situations. Involving experts with experience in implementation and technological audit in the project may increase the chances of professional assessment and maintaining the operational continuity of the designed system.

Technological integration

In order to minimize the risk, it is recommended to optimize the parameters of the algorithm behind the QR code generator and create a robust training and test sets that highly reflect reality to eliminate potential problems related to incorrect coding or reading. Additionally, it is recommended to conduct extensive tests on a variety of devices with different operating systems, which will allow for comprehensive verification of the system's operation and ensure its compatibility and reliability in various conditions of use. The use of technologies that support all web browsers is crucial to ensuring a consistent and optimal appearance and functionality of the project regardless of the browser chosen. In addition, conducting numerous technical tests is necessary to ensure high quality of the project. The use of technology enabling the development of the solution on multiple mobile platforms will assure wide availability of the solution and will increase its adaptability.

Risks dependent on internal factors

Recommended actions aimed at minimizing risk and ensuring the stability of the system include involving the entire team in the data development process, as well as conducting numerous partial tests to systematically verify individual project elements and identify potential problems before their escalation. Employing high-class specialists will enable effective management of the complexity and technical requirements of the project. The use of the highest quality raw materials from reputable manufacturers, adapted to the latest printing technologies, will minimize the risk of QR code reading errors. Implementing cloud solutions in the event of a failure will ensure the security and reliability of the IT infrastructure and eliminate the risk of downtime and data loss. Also, the ability to switch the website domain to a server from a cloud platform - even when disconnected from the main network - will ensure the solution's resistance and secure its uninterrupted operation.

These recommended actions constitute a comprehensive set of preventive measures aimed at minimizing risks. They ensure stability and reliability during designing innovative product authenticity safeguards based on QR codes.

Conclusion

Ten essential risks associated with the design and implementation of innovative product authenticity safeguards based on QR codes have been identified. These risks were then analyzed using a risk assessment matrix, which is widely recognized as the starting point for risk measurement and assessment. The analysis showed that one of the risks, namely risk no. 10 "Server failure and/or network failure", is in the red zone, which means the highest level of threat and the need to apply the most urgent remedial steps. Two risks (risk no. 3 "Emergence of new technological solutions" and risk no. 9 "Not all mobile devices will be able to support the application") are in the yellow zone, indicating a moderate level of threat requiring close monitoring and possible corrective actions. The remaining seven risks were in the green zone, which means a low level of threat and a relatively low probability of their occurrence.

Further thematic grouping of the identified risks indicated four key areas: competition, external websites, technological integration and risks dependent on internal factors. The first three areas are characterized by a low level of risk, while risks dependent on internal factors have an average risk level. This means that the design and implementation of innovative safeguards for the authenticity of products based on QR codes can be implemented, but in a controlled manner, and relying on a thorough risk analysis enables to take adequate preventive and corrective actions.

The risk matrix, although it constitutes a simple method, is therefore not only a practical tool for visualizing risks, but also the basis for making informed management decisions. However, it should be borne in mind that risks may change over time, therefore the risk matrix may need to be updated frequently to remain current and useful in a dynamically changing technological environment.

Overall, this systematic approach not only aids in preventative and corrective measures that can be introduced for the success of the innovative project, but also allows for scientifically driven decision-making in a technological landscape that is in constant flux.

Credit Authorship Contribution Statement

Both authors play equal roles in the research and development of the project, including the analysis, writing, and decision-making processes. Their contributions were collaborative and evenly distributed throughout the study.

Acknowledgments/Funding

This work was co-financed by the Silesian Entrepreneurship Center (ŚCP) RPSL.01.02.00-24-070B/16 and presents partial results of a research project entitled "Q-Code: R&D works in the field of protecting the authenticity of valuable products" carried out by ETICOD sp. z o.o.

Conflict of Interest Statement

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

[1] Aulia, M. M., Saha, N., & Rahman, M. M. (2024). Protected QR Code-based Anti-counterfeit System for Pharmaceutical Manufacturing. ArXiv, 1-6. https://doi.org/10.48550/arXiv.2404.07831

[2] Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253, 1-13. http://dx.doi.org/10.1016/j.ejor.2015.12.023

[3] Bansal, D., Malla, S., Gudala, K., & Tiwari, P. (2013). Anti-Counterfeit Technologies: A Pharmaceutical Industry Perspective. *Scientia Pharmaceutica*, 81(1), 1 - 14. https://doi.org/10.3797/scipharm.1202-03

[4] Berglund, H. (2007). Risk Conception and Risk Management in Corporate Innovation: Lessons from two Swedish Cases. *International Journal of Innovation Management*, 11(4), 497-513. https://doi.org/10.1142/S1363919607001849

[5] Deptuła, A.M. (2024). Assessment Criteria of Innovations Risks: Analysis of Research Results. *Journal of the Knowledge Economy*, 1-17. https://doi.org/10.1007/s13132-023-01659-1

[6] Deptuła, A. M., & Knosala, R. (2015). Risk assessment of the innovative projects implementation. *Management and Production Engineering Review*, 6(4), 15-25. http://dx.doi.org/10.1515/mper-2015-0032

[7] Gorokhovatskyi, V., Sergienko, O., Sosnov, I., Tatar, M., & Shapran, E. (2021). Risk Assessment of Innovative Projects: Development of Forecasting Models. [in:] Guryanova, L., Yatsenko, R., Dubrovina, N., & Babenko, V. (eds.), Machine Learning Methods and Models, Predictive Analytics and Applications. Proceedings of the Workshop on the XIII International Scientific Practical Conference Modern problems of social and economic systems modelling (MPSESM-W 2021), Kharkiv, Ukraine, 2927, 18-37.

[8] Huo, L., Zhu, J., Singh, P. K., & Pavlovich, P. A. (2021). Research on QR image code recognition system based on artificial intelligence algorithm. *Journal of Intelligent Systems*, 30(1), 855-867. https://doi.org/10.1515/jisys-2020-0143

[9] Karrach, L., Pivarčiová, E., & Božek, P. (2020). Identification of QR Code Perspective Distortion Based on Edge Directions and Edge Projections Analysis. *Journal of Imaging*, 6(7), 67-86. https://doi.org/10.3390/jimaging6070067

[10] Kovačević, N., Stojiljković, A., & Kovač, M. (2019). Application of the matrix approach in risk assessment. *Operational Research in Engineering Sciences: Theory and Applications*, 2(3), 55-64. http://dx.doi.org/10.31181/oresta1903055k

[11] Li, D., Gao, X., Sun, Y., & Cui, L. (2017). Research on Anti-counterfeiting Technology Based on QR Code image Watermarking Algorithm. *International Journal of Multimedia and Ubiquitous Engineering*, 12(5), 57-66. http://dx.doi.org/10.14257/ijmue.2017.12.5.05

[12] Murray, S.L., Grantham, K., & Damle, S.B. (2011). Development of a Generic Risk Matrix to Manage Project Risks. *Journal of Industrial and Systems Engineering*, 5(1), 35-51.

[13] Nasr, O. A., Alsisi, E. A., Mohiuddin, K., & Alqahtani, A. M. (2023). Designing an intelligent QR code-based mobile application: A novel approach for vehicle identification and authentication. *Indian Journal of Science and Technology*, 16(37), 3139-3147. https://doi.org/10.17485/IJST/v16i37.1389

[14] Pawar, A., Fatnani, C., Sonavane, R., Waghmare, R., & Saoji, S. (2022). Secure QR Code Scanner to Detect Malicious URL using Machine Learning. [in:] *2nd Asian Conference on Innovation in Technology* (ASIANCON), 1-8, https://doi.org/10.1109/ASIANCON55314.2022.9908759

[15] Petrova, K., Romaniello, A., Medlin, B.D., & Vannoy, S.A. (2016). QR Codes Advantages and Dangers. [in:] Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016), 2(ICE-B), 112-115. http://dx.doi.org/10.5220/0005993101120115

[16] Picard, J., Landry, P., & Bolay, M. (2021). Counterfeit detection with QR codes. [in:] Proceedings of the 21st ACM Symposium on Document Engineering (DocEng '21), 16, 1-4. https://doi.org/10.1145/3469096.3474924

[17] Vaithilingam, S., & Shankar, S. A. M. (2024). Enhancing security in QR code technology using AI: Exploration and mitigation strategies. *International Journal of Intelligence Science*, 14, 49-57. https://doi.org/10.4236/ijis.2024.142003

[18] Walas-Trębacz, J., & Bartusik, K. (2023). Identification of risk types in innovation projects. *International Journal of Contemporary Management*, 59(4), 74-93. http://dx.doi.org/10.2478/ijcm-2023-0013

[19] Wang, T., Zheng, H., You, C., & Ju, J. (2023). A Texture-Hidden Anti-Counterfeiting QR Code and Authentication Method. *Sensors*, 23(2), 795, 1-25. https://doi.org/10.3390/s23020795