

MANAGEMENT AND BUSINESS MODEL RISK PROFILE
IN SECURITY SYSTEMS DEVELOPMENT

Valeri Panevski

Received on February 7, 2024

Presented by Ch. Roumenin, Member of BAS, on February 27, 2024

Abstract

The business model applied in the development of security systems by scientific organizations, independently or in terms of key partnerships with higher education institutions and business organizations structured through competence centres, are part of their strategic assets. But in managing this business model, both planned and unforeseeable risks may arise, which determines the need to develop a business model risk framework.

The author's experience in structuring a business model risk framework for the development of security systems by scientific organizations is the basis of the present publication.

Key words: business model, risk profile, security systems

Introduction. When we talk about good management practice for ensuring the security of the organization, it is necessary to mention the internationally accepted method for business continuity management (BCM). BCM encompasses the policies, capabilities and approaches that an organization uses to ensure the

This paper is the result of implementation of the scientific work of the author, as a part of the IMSETCH-BAS team, participating in Work Package 2. "Intelligent security systems", Project BG05M2OP001-1.002-0006 Competence Center "Quantum Communication, Intelligent Security and Risk Management Systems (Quasar)", funded by the European Regional Development Fund through the Operational Programme "Science and education for smart growth", co-financed by the European Union through the European Structural and Investment Funds.

<https://doi.org/10.7546/CRABS.2024.04.12>

continuity of its business operations during and/or after a disruptive event [1, 2]. This process is tailored to organizational specifics based on mission, business model and available assets.

At the same time, appropriate application of the Business Model (BM) is the basis of organizational strategy and competitiveness and is based on the analysis of the components of the organization by considering the assets created, the resources used, the plans developed and the establishment competences.

As strategic assets, BMs define the logic by which the organization transforms produced goods and services into earnings [3]. In this regard, business continuity implementation focuses on ensuring continuity by increasing the resilience of the assets through which a particular BM is implemented.

Last but not least, BMs must adapt in response to contingencies related to risk events arising from natural disasters, man-made disruptive impacts, and also to the technology-driven innovation. This is of particular importance to scientific organizations whose scope of research includes the development of security systems.

Business continuity management of the organization. The internationally accepted BCM process is a summary of best business practices based on the standards, developed by technical committee ISO/TC 292 “Security and resilience” of the International Organization for Standardization (ISO), which offer a solid foundation for organizational flexibility in adapting to change.

What are the risks to business continuity management?

Risks or business continuity events are the most common events that can disrupt an organization’s operations and can be natural or man-made crises. Determining these risks is a vital part of business continuity planning, namely: weather; natural disasters; a physical threat to security; assigning a product of the organization; supply chain issues; threats to personnel and employee safety; technological incidents in the organization’s facilities; destruction of facilities or property of the organization; power outages; server crashes; failures in public and private services; environmental disasters, including spills of hazardous materials; network outages; human mistake; stock market crashes; cyber attacks and hacking activity.

Every single one of these challenges can lead to bigger problems for an organization, namely: staff injury; equipment damage; causing brand damage and loss of income and net worth. BCM and planning process address and reduce the impact of these contingencies on the organization, including the operating business model.

Business model for the security systems development. Generally, the BM framework can be defined as positive and useful management form, which also helps to consider approaches to develop new and/or optimize the characteristics of existing security systems as well as their elements. This applies to the security system model (SSM) developed within WP2, as well as related software and hardware.

With regard to the elements of the BM, it is clear that the price offer and the client segment are the most important for generating BM for developing the SSM. Another element considered important is the key partners. For example, an aspect that appeared during the development was the possibility of framework contracts with business organizations in the national defense industry, as well as participation in projects under the Research and Innovation (R&I) programme Horizon Europe 2021–2027. The SSM concept is related to areas such as supply chain, production management and marketing and is an important solution for the strategic positioning of the QUASAR project, whose guide intends to develop and improve the SSM, for example, to strengthen its own brand or to become a developer who will renew the scientific organization that the SSM develops.

But BM, developed on the basis of established contemporary trends and good practices, is just the tip of the iceberg of things. In order to function properly, it is necessary to own a Business model risk profile framework.

Business model risk profile framework. There is a need in various areas of business to develop a better understanding of BM risks, taking into account the fact that they are the business plans used by the organization to create, deliver and acquire value. An adequate risk framework would support the full range of risk management capabilities, namely identifying key risks, quantifying and managing those risks.

The need to improve BM risk management also stems from the different spheres of economic activity, since business models are the basis of every organization. Last but not least, the challenge of determining the business risk profile stems not only from the lack of a commonly accepted definition of what constitutes BM, but also from the lack of methodologies to determine the exact impact of the competitive landscape characterized by competing BMs.

Therefore, when developing an organization's BM, it is necessary to create a better understanding of the risks associated with the development and implementation of BM. The proposed risk identification framework (Fig. 1) would improve the ability to manage potential risks [4].

There are various publications presenting the risk profile in the development of BMs, as a basis for determining the risk profile in the present study the concept presented in the "Open Risk Manual" was applied [5].

Risk profile framework short description.

Customer segments. A customer segmentation becomes a risk when it no longer optimizes the reality of the client base or how the internal structure of the organization corresponds to this client base. The impact of such a mismatch will be down the chain as ineffective or inappropriate distribution, reduced product attractiveness, etc., which will ultimately affect revenue. Assessing the risk of inappropriate segmentation requires an analysis of current and historical patterns of behaviour and customer expectations.

Designed for MISSD/WP2 QUASAR	Designed by WP2 team	Date 2021-11-04	Version 1.0	
Risks Profile				
Key Partners	Key Activities	Value Proposition	Customer Relationships	Customer Segments
- refusal of the partnership by external party with difficulty in replacing it with another party - the partnership fails to deliver the expected results, creating a negative reputation or negative impact on costs	- activity: poor or incorrect performance of regular business tasks - performance: unfavorable development of the circumstances for the staff fraud: unexpected loss as a result of deceptive activities Key Resources - legal risks: - physical assets risks - risks for key personnel - employment practices risk - financial assets risks - financing risks	- problems with the provision of services (quality control) - changing customer expectations - changing the economic environment - availability on the market of alternative products or services	- internal or external factors that negatively affect the relationship (damage to reputation, poor performance) - unexpected connection support costs increase Channels - quality of the used sales channel (people, processes, equipment) - suitability for changing behavioral patterns (new more attractive channels) - oversaturation of the channel scope by other competitors	- customer segmentation no longer optimally reflects the reality of the customer base - the change in customer behavior and expectations
Cost Structure			Revenue Streams	
- variable costs to be higher than expected - dependence on any of the elements of the business model (eg relying on a partner for a specific resource), adverse events can generate large jumps in costs			- change in the size of the market: reduction of the wider market demand for products and services of the organization as a result of external factors - change in market share: reduction in sales volumes will lead to unexpectedly lower revenues - price risk: lower profitability compared to the business plan as a result of stricter prices	

Fig. 1. BM risk profile framework

Value proposition. There is an expected value level that accumulates the customer using the product or service. The risk is that the actual valuable proposal is seriously reduced or not materialized, leading to customer loss or inability to attract new customers.

Channels. The intended distribution channels are expected to be working. The risk is that distribution channels may become ineffective and cannot achieve their goal (even while requiring running costs to maintain).

Customer relationships. The organization has planned to create and maintain a particular set of customer relationships (supported by resources and activities). The risks relate to the impact of internal or external factors that have a negative communication, thus creating hindrances to achieving the planned goal (reputation damage, poor performance) or an unexpected increase in cost support.

Revenue streams. The revenue is expected to be sufficient to cover all expenses and to provide a profit margin. Deviations from this expectation (leading to unprofitability in the organization's activity and even insolvency) are risks to revenue. Revenue risks are materialized through missed sales targets (volumes) or inability to maintain prices.

Key resources. The necessary resources should be available to those interested and should contribute to the completion of the planned tasks. The risks manifest themselves as awareness that this is not fulfilled

Key activities. It is expected that there are enough resources to allow the necessary activities to be performed during the planned period. The risks are when key resources are not provided.

Key partners. A list of partners has been prepared that is expected to deliver critical resources or activities. Partnership risks include unexpected developments of relationships that deviate from the partners' agreement (providing activities or delivery of resources).

Cost structure. An estimated structure of the expected costs is planned, which takes into account current and observed cost levels. A major risk factor related to the cost structure is that variable costs will be greater than expected. In turn, higher variable costs may depend on: higher compensation levels due to labour market conditions; external market prices for resources or services, etc.

In addition, we should not forget competition is the factor that increases the risk profile of any BM, drawing attention to all its elements. The existing level of competition and the relevant distribution of market share must be included in the business plan as expected. Uncertainty is related to adverse (for organization) development of the ability of existing or new competitors to increase market share or to work more profitably.

The presented analytical framework for systematic identification of the risks of BM indicates the main risks identified so far (Fig. 1). In the process of developing and improving the security system, the BM Risk Profile Framework content will be updated according to the palette of emerging and/or dropped risks.

Some dependencies between business continuity management and business model risk profile. To ensure the general process of preparing the BM risk framework for the development of intelligent security systems it is of great importance for the organization "... to be able to continue to deliver products and services at an acceptable predefined capacity ..." (item 1 "Scope", item "c") [6].

Information about the critical elements (critical assets) of the business model is most effectively obtained through Business Impact Analysis (BIA). "BIA enables the organization to assess the impact of disruption of activities would have on delivery of its products and services. This enables the organization to prioritize the resumption of activities." (item 8.1.2) [6].

One of basic dependencies is the link between the risk assessment item 8.2. "... to enable the organization to assess the risks of prioritized activities being disrupted so that it can take appropriate activity to address the risks" [4] and "Customer Segment", "Key Activities" and "Key Partners" from the Business Model Risk Profile framework.

Through the properly implemented risk assessment process, it is expected to achieve prevention against possible risk events related to these elements, namely "For identified risk required treatment in line with the overall attitude of risk, the organization should consider ways for reducing the likelihood..." (item 8.3.2.4) [6].

Conclusions. The information presented provides a brief overview of the developed BM risk profile framework for managing studies across the developed SSM options in WP2 of the QUASAR project.

The approach used is based on the modern experience of business organizations that have achieved high efficiency in marketing their production list and the ISO/TC 292 "Security and resilience" standards in the field of BCM.

There are many compelling reasons for an organization to develop its own BM and, as a result, to implement process innovations. The existence of BM usually requires a fundamental change in the way the organization works and thinks and the associated possible risks, which is why the application of ISO standards in the field of BCM in determining and managing risks for BM elements has an extremely high potential for sustainable increasing competitiveness and success.

Determination of the characteristics of dangerous events and the assessment of their consequences and probabilities require an integrated framework capable of incorporating different analysis methods to capture the problem from different characteristic points of view related to their topology and properties – functional, logical and dynamic. This approach, adopted in the structuring and functioning of the BM risk framework in the conditions of the application of the business continuity management, is expected to represent the real competitive advantage of the cooperation between scientific organizations, universities and industrial organizations in the development of models of security systems in the development of security system models.

REFERENCES

- [1] STOICHEV K., D. DIMITROV, V. PANEVSKI (2016) Physical Protection Technologies, Systems and Equipment, Sofia, Publishing House of the University of National and World Economy, ISBN:978-954-644-810-1, 250 pp.
- [2] DIMITROV D. L. (2019) Standardized approaches to the integration of critical infrastructure management systems, Proceedings, Security, Vol. III, Scientific Technical Union of Mechanical Engineering “Industry-4.0”, ISSN 2535-0315 (Print), ISSN 2535-0323 (Online), 239–241.
- [3] ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements.
- [4] PANEVSKI V. (2022) A variant of the risk profile of a business model in the development of intelligent security systems, Security & Future, **6**(1), 7–10.
- [5] PAPADOPOULOS P. (2016) Open Risk White Paper: Identification Framework for Business Model Risks, 19 pp, https://www.openriskmanagement.com/wp-content/uploads/2016/02/OpenRiskWP05_010916.pdf.
- [6] ISO 22313:2020 – Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301.

Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A. Balevski”, Bulgarian Academy of Sciences, 67 Shipchenski Prohod Blvd, 1574 Sofia, Bulgaria
e-mail: panevski@ims.bas.bg