



Viable IT Risk Management System by Viable System Model (VSM): Action Research for Managing IT-related Risk in the Banking Service

Ali Akbar Arghand¹

Accepted: 19 November 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

In recent years, some standards and frameworks proposed the risk management structures for managing and controlling IT risk that is the main component of enterprise governance of IT. Unfortunately, these frameworks have a retrospective view of threat analysis and less pay attention to future threats in the business environment, and do not propose adaptable solutions. At the same time, the current risk framework is not based on a strong scientific system modeling. In this research, the researcher proposed the Viable System Model (VSM) as an adaptable and comprehensive framework that is based on scientific modeling with the systematic approach for managing and controlling IT risk in today's complex business environment. This research did in a systematic action research methodology in the banking context in Iran. The results showed that by applying the VSM as a framework for managing IT risk, adaptability of IT risk criteria according to the future threats can be achieved by this framework. A comprehensive risk management framework (retrospective and prospective view) with a systematic approach could be achieved by this system modeling.

Keywords Viable IT Risk Management system · VSM · Enterprise Risk Management (ERM) · IT governance · IT risk · Banking services

Introduction

The development of new technologies in IT caused the increased complexity of this field in recent years. Due to this complexity, the risk related to IT becomes more critical and if these risks ignored, it could be dangerous for achieving business objectives. Nowadays, IT risk management system became the main concern of senior managers of organizations. Meanwhile, many organizations that have not a good understanding of IT risk management systems have spent a lot of money to reduce IT risks, but they just waste their money and not successful in managing the IT risks. "*Many organizations*

✉ Ali Akbar Arghand
aliakbararghand@yahoo.com

¹ Department of IT Management, Science and Research Branch of Islamic Azad University, Tehran, Iran

struggle with risk assessment and some believe that it shouldn't be practiced at all! Many do some form of risk assessment, but often badly, or incompletely. Some just don't bother, preferring an approach which relies on standards and baselines to manage the common risks, some just ignore the problem and trust to hope. (Coles and Moulton 2003)".

"Today, it is clearly acknowledged that Information Technology (IT) is no more only a technical issue. Thus, the complexity and importance of IT in companies involve a necessary governance layer. Such a governance layer generally encompasses risk management and compliance as steering tools. This evolution has implied the adoption of a new paradigm in IT" (De Smet and Mayer 2016).

Risk is a combination of the probability of an event and its impacts (negative and positive) in business, which is usually referred to as the negative impacts that could be affected the business goals. *Information Security Risk (ISR) is define by ISO 31000 as "a combination of two factors: probability and consequences. It asks two basic questions: what is the probability that a particular information security event will occur in the future? And what consequences would this event produce or what impact would it have if it actually occurred? Information security risks often emerge because potential security threats are identified that could exploit vulnerabilities in an information asset or group of assets and therefore cause harm to an organization" (Fazlida and Said 2015).*

IT risk management is one of the main components of IT governance. Efficient and effective risk management needs an adaptable framework based on scientific concepts and foundations. IT risks management consists of the processes such as risk identification, risk assessment, risk analysis, risk evaluation, risk response, risk monitoring, and reporting. In recent years, some standards and frameworks have been developed such as the framework of Risk IT (by ISACA), ISO 31000, COSO, ISO 27005, but none of them proposes a solution for the adaptability of the framework to deal with changes (and its risks) in the business and IT environment.

Today's ever-changing business environment causes changes in business and IT strategy and this causes changes in IT-related risk plan to align and integrate IT risk with enterprise risk. Therefore, an adaptable IT risk framework can predict the changes and related risks then compare and balance between current and future risk so propose the new risk plan according to those changes.

Because of the complexity in IT and business environment, IT risk managers have faced an ill-structured situation when they want to manage IT risk. Applying soft system methodologies such as the viable system model can be a good choice to manage this complexity. The VSM, which is based on strong scientific sciences such as open system theory, and cybernetic approach, can be helpful to deal with changes in business and IT related risk complexity. According to these benefits, IT managers have used this soft system modeling in recent years in IT governance framework and in information security management system.

Although in recent years some standards and frameworks such as NIST, ISO, ISACA (Isaca 2009) have been proposed for IT risk management but none of them have been developed based on strong scientific concepts and have not provided a clear mechanism for adaptation to the complex IT environment. In this study, the researcher used VSM as an adaptable framework for managing IT risks in the banking context.

Background

Stafford Beer, known as the father of management cybernetics, developed a model based on organizational cybernetics in his books. Organizational cybernetics is a powerful system approach formulated for steering complex systems in a turbulent environment. Feedback, variety and black boxes are the main cybernetic concepts used by Stafford Beer (Beer 1972, 1979; Beer and Beer 1985). Stafford Beer used the viable system modeling for the first time in 1970 at the invitation of Chilean leader Salvador Allende to model socio-economic modeling in the country.

According to Beer, the cybernetic concepts of a black box, negative feedback and variety, are ideal for helping us to understand and improve complex systems, like organizations, that are characterized by extreme complexity, self-regulation, and probabilism (Jackson 2005). Viable system modeling should be considered one of the most powerful tools in the study of organizational structures (Espejo et al. 1999). "A social system is viable if, and only if, its structure fulfils a number of requirements, which the theory specifies. Concretely, according to the model, a viable organization must dispose of five managerial subsystems and their interrelationships, as set forth by the theory: (1) System 1. Management of a basic subsystem. (2) System 2. Coordination of subsystems, attenuation of oscillations between them. (3) System 3. Operative management of a collective of subsystems.

(4) System 3*. Auditing and monitoring channel. (5) System 4. Management for the long term, relationships with the overall environment. (6) System 5. Normative management, corporate ethos (Schwaninger 2006)". Figure 1 shows the VSM subsystems. As can be seen in Fig. 1, subsystem 1 (operations unit) is related to the main primary services of the company, which is responsible for the production and delivery of goods. Subsystem 2 is responsible for coordination in the organization. Subsystem 3 is responsible for daily management of the system. Subsystem 3* plays the audit role to help system 3 to evaluate the performance of system 1. Subsystem 4 is responsible for adaptability and track the external environment. Subsystem 5 is also responsible for determining the identity of the organization and creating a balance between current management (subsystem 3) and future management (subsystem 4).

Markus Schwaninger and Christine Scheef in a study in 2016 did research about testing the VSM model. Their article's purpose is to test the theory empirically, on the grounds of a broad survey and pertinent quantitative analysis. The collected data support the hypotheses and therewith corroborate the theory of the VSM (Schwaninger and Scheef 2016). Vahidi, Aliahmadi and Teymouri did research in 2019 about the trend of cybernetics and VSM. Table 1 shows the management cybernetics evolution (Vahidi et al. 2019).

The Application of Viable System Model (VSM) in IT governance

The importance of IT governance in achieving the business goals in recent years, convincing researchers to focus on the applicability of VSM as a strong scientific foundation and a reliable soft system model for the IT governance framework.

One of the first articles of using VSM in IT governance is related to Peppard in 2005. By using Ashby variety Law, cybernetic approach, and VSM, he introduced a framework for IT governance for IT operations and IT projects (Peppard 2005). Figure 2 shows his proposed model.

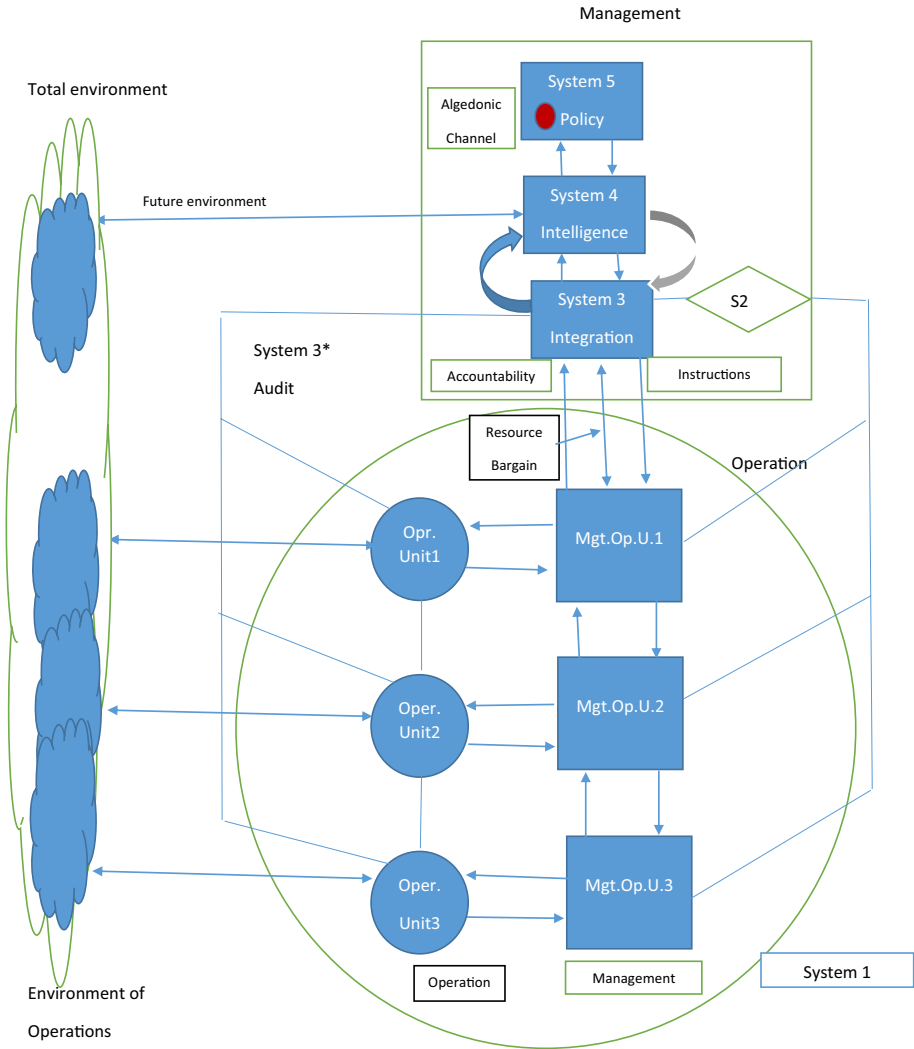


Fig. 1 The viable system model (Jackson 2005)

In 2008, Rakers and Rosenkranz proposed VSM for a management project in designing and implementing data ware house project in the financial field (Rakers and Rosenkranz 2008). In 2009, Lewis and Millar proposed the VSM for Governance Viable Mode (VGM) for IT governance (Lewis and Millar 2009). Figure 3 shows their VGM model. In 2018, the Huygh and De Haes used VSM for IT governance in a case study in a human resources company in Belgium (Huygh and De Haes 2018).

In 2020, De Haes et al., addressing the importance of applying the VSM in viable IT governance, in a part of their book (De Haes et al. 2020).

In 2021, Arghand, Alborzi and Rajabzadeh did a research and use VSM in designing data center (Arghand et al. 2021).

Information security experts also considered the applicability of VSM in information security. In 2004, Gokhale and Banks proposed this model for information security systems.

Table 1 The evolution of management cybernetics (Vahidi et al. 2019)

Year	Scholar	Concept
1959	Beer	Cybernetics and Management
1962	Beer	Cybernetic factory
1966	Beer	Decision and Control in Cybernetics
1972	Beer	Brain of the firm
1974	Von Foster	Second order cybernetics
1979	Beer	Heart of Enterprise and creation of VSM
2001	Reyes	Second order cybernetic in VSM
2004	Schwanger	Needs for combination of VSM, SD, and others
2004	Yolles	VSM and Agency Theory relationship
Now days	Various Researcher	Application of VSM

According to the capabilities of the VSM subsystems, they proposed this model as a suitable option to deal with cyber threats (Gokhale and Banks 2004). In 2002, Hutchinson and Warren

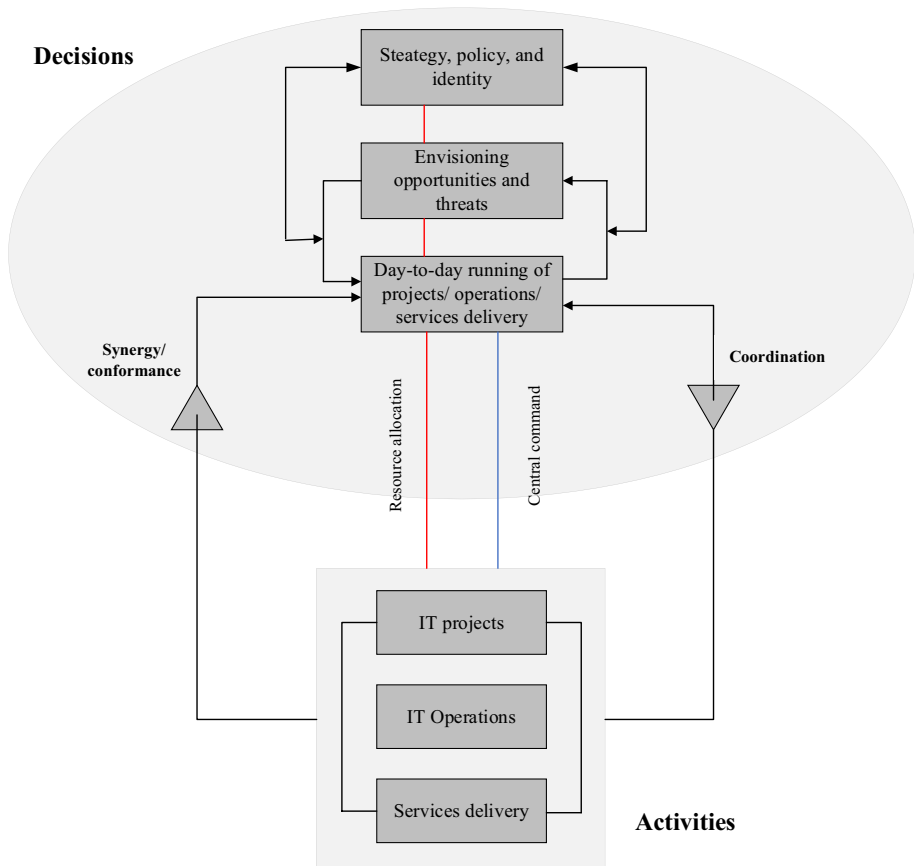


Fig. 2 IT governance model (Peppard 2005)

introduced VSM as a suitable tool for diagnosing and analyzing information security systems in organizations (Hutchinson and Warren 2002).

In 2013, Alqurashi Wills and Gilberts did a study in this field. They used the VSM for IT security governance. They pointed out that a viable system model of information security governance (VSMISG) can be used as a suitable framework to help organizations to ensure effective internal control as well as a tool for business continuity in organizations. (Alqurashi et al. 2013). In 2017, Goldes and et al. used the VSM for information security and compare it with other standards and security frameworks such as COBIT, NIST, ISO. They founded that all the benefits of these frameworks are included in the VSM (Goldes et al. 2017). In 2014 in a study, Spyridopoulos et al. applied the VSM for managing cyber security risk in industrial control systems (Spyridopoulos et al. 2014).

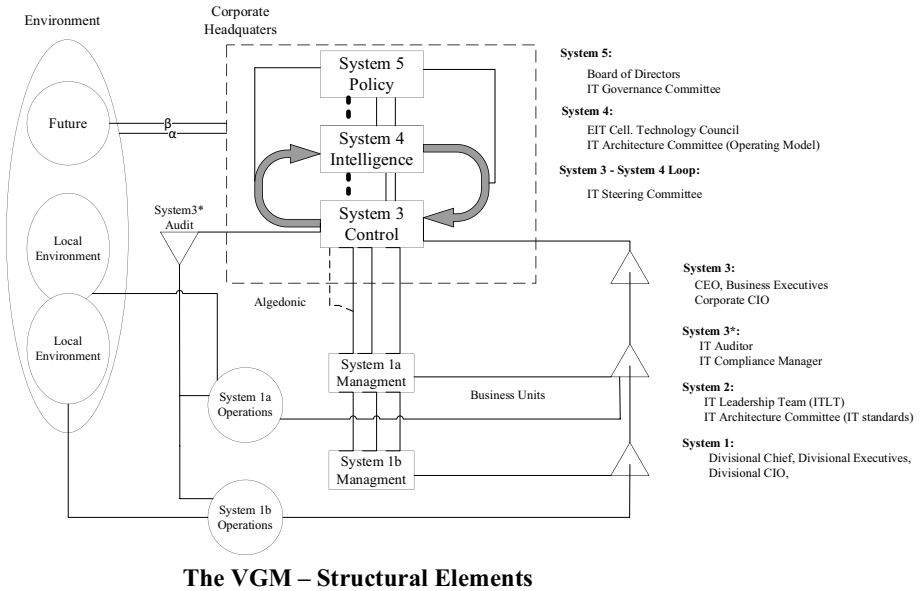
In recent years, some studies have been conducted for applying the VSM to IT management system and information security, but fewer efforts have been done to apply VSM for IT risk management system. In this research, we focus on the applicability of the VSM as an adaptable framework for IT risk management system.

Methodology

This research has been done with a systemic approach presented by Checkland & Holowell (Checkland and Holwell 1998). Systemic action research method includes four step. 1- Determining the framework of ideas and methodology, in this research is the use of VSM as an adaptable framework for IT risk management system. 2- Determining the area of concern, in this research the use of viable IT risk management in the e-banking services. 3 Using the methodology, in the research, researcher used the VIPLAN methodology which was presented by Espejo, Bowling, and Hoverstadt (Espejo et al. 1999) as a well-known methodology in the field of VSM. Figure 4 shows the research methodology. Data collected using research literature, library studies and using field observation tools, interviews, and document review. An expert team was formed to study (collect, evaluate, and respond) the status of the current and future of IT-related risk. The team consisted of some employees who served on the front lines of the services (act as system 1) to study the current status of IT risks and also some IT experts for analyzing the future state of IT risk related to the future of banking services (act as system 4). The researcher, as a member of the team, was responsible for collecting and integrating all risks related to the current services and with the help of the IT operational manager and IT risk officer (who were the team members and act as system 3) build the current IT risk profile. By combining the current IT risk profile (system 3) and the future IT risk profile (system 4), a new and adaptable IT risk strategy and roadmap emerged that aligned and integrated more and better with the enterprise risk manager (ERM). These e-banking risks consist of IT infrastructure and application risks.

Findings

To design and diagnose the IT risk management system based on the VSM, first, it is necessary to identify a conceptual framework of viable IT risk management (Fig. 5). This framework is compared to risk IT framework which is presented by ISACA in



The VGM – Structural Elements

Fig. 3 The VGM model proposed by Lewis and Millar (Lewis and Millar 2009)

2009 (Isaca 2009). As you can see in this figure, we can separate IT risk Governance (system 5) and IT risk management (system 4, 3, 2, 1) into two distinct parts.

IT risk governance (system5), which has the most authority in the system, defines, evaluates, and monitors the overall policies and objectives of risk related to IT and

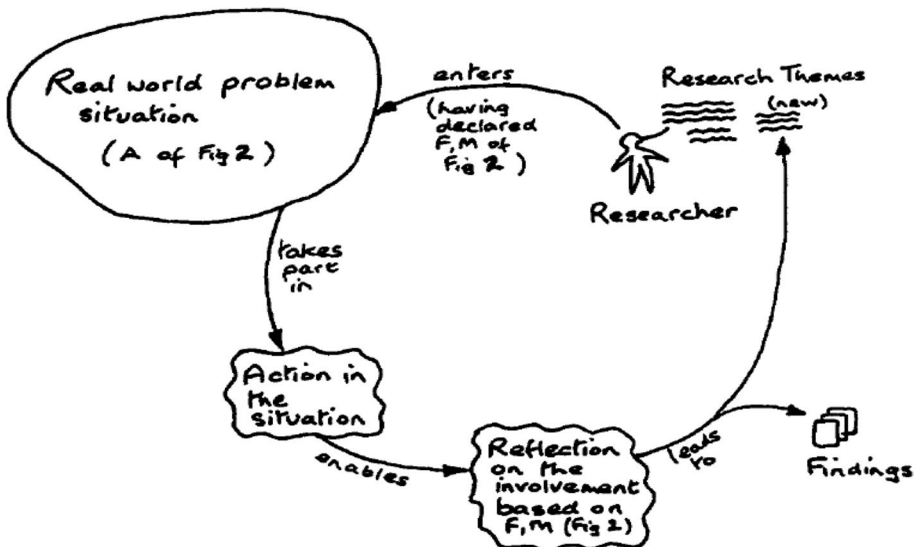


Fig. 4 Systemic action research (Checkland and Holwell 1998)

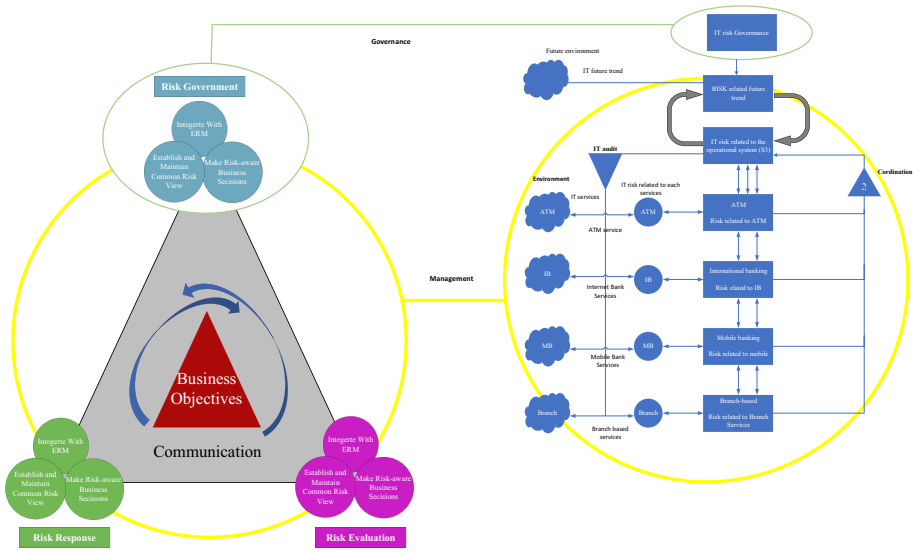


Fig. 5 Conceptual framework for viable IT risk management system by VSM compared to IT risk framework presented by ISACA 2009

establishes a common risk view in the system and ensure that IT risk is integrated with ERM. This system also ensures that IT risk management processes are embedded in the enterprise.

IT risk management (system 4, 3, 2, 1) translate the IT risk goals, which are established by the IT risk governance (S5 that is responsible for establishing an IT risk framework, promoting risk cultures, overall risk policies, propose and approve risk appetite and risk tolerance, ensuring integration with ERM ...) into programs, projects, and actionable activities.

For designing the subsystems of the VSM, at first we should identify the scope of the system, which we want to start IT risk processes.

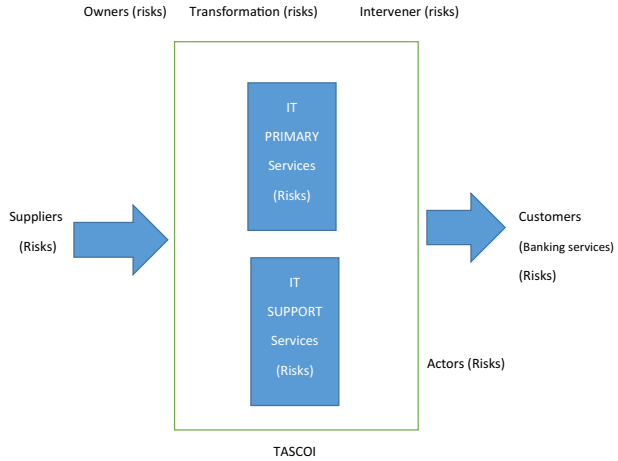
Step 1: Identify the IT Risk Management System

To identify the IT-related risk in any organization, we should first determine the system and the context that we are trying to examine the risks in that system. The primary IT services, support IT services, the organization’s business context, IT goals and programs, the scope of the IT system, the boundaries of the system, IT service owners (who are the risk owner), and the stakeholders. In this section, which is inspired by the VIPLAN, the main components of the system are specified.

To identify the system, the TASCOI method is used. In this research which was done in the banking context (for e-banking services), we identify this step as Fig. 6.

As can be seen in Fig. 6, in our IT system, which is related to the e-banking services, the primary services are those that create direct value (service) to customers such as ATM services, POS services, Internet banking services, mobile banking services, and the support IT services are those that support primary services and do not create direct value to customers (such as data centers and IT infrastructure). IT risk consists of the risks related

Fig. 6 Identify the IT system in the banking context



to the IT operation, risks related to IT programs, and the risks related to IT strategies. In this research, we focus on the risks related to IT operations.

Now we can design the VSM subsystems based on the IT service operation.

STEP2: Designing S1-S5

According to the results of step 1, we design the VSM subsystem.

Designing S1 (Risk Related to IT Services)

To study IT risk related to operational units (S1) based on VSM, we can chunk each primary service (applications) into operational services. The responsibility of these units is identifying the risks, analyzing the risks, evaluating the risks, selecting the risk response, monitoring and reporting the status of risk profile. The employees who are responsible for the services and work in the front line are the best choice for examining the status of IT risk.

Figure 7 shows how to design S1 for identifying IT related risk. The risk related to mobile banking services, ATM services, POS services, internet-banking services, and branch-based services identified as operational IT-related risks for each service (S1). To integrate the holistic nature of IT risk, the subsystems should communicate together. Figure 7 shows the design of this subsystem for our research. Collecting data, analyzing risk, maintain risk profile, articulate risk, monitor risk, and react to risk are the responsibility of system 1.

When a risk is detected by each operational unit and is very critical, and can endanger the whole system, the operational units should alert the senior managers via an algedonic channel.

Designing S2 (Coordination of IT Risk Subsystems)

Establishing an integrated and coordinated environment and a shared understanding of how IT risk is analyzed and report between all units is the responsibility of S2. Coordination help the system to seek to ensure that the autonomy granted is the maximum possible

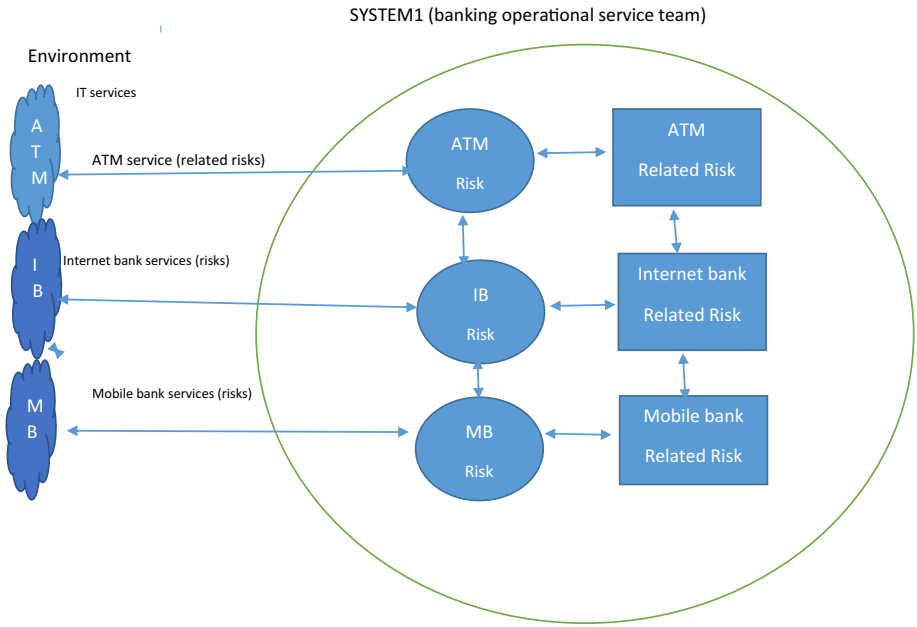


Fig. 7 Designing S1 for e-banking IT related risk

subject only to the whole continuing to exist. This subsystem provides standards, policies, procedures, and work instructions of IT risk for system 1 to maintain a coordination of IT risk between each subsystem 1. For example, providing some policies and procedures for the assessment and reporting of IT risk at specific intervals and according to some standards or frameworks is the responsibility of system 2. Figure 8 shows the S2 design.

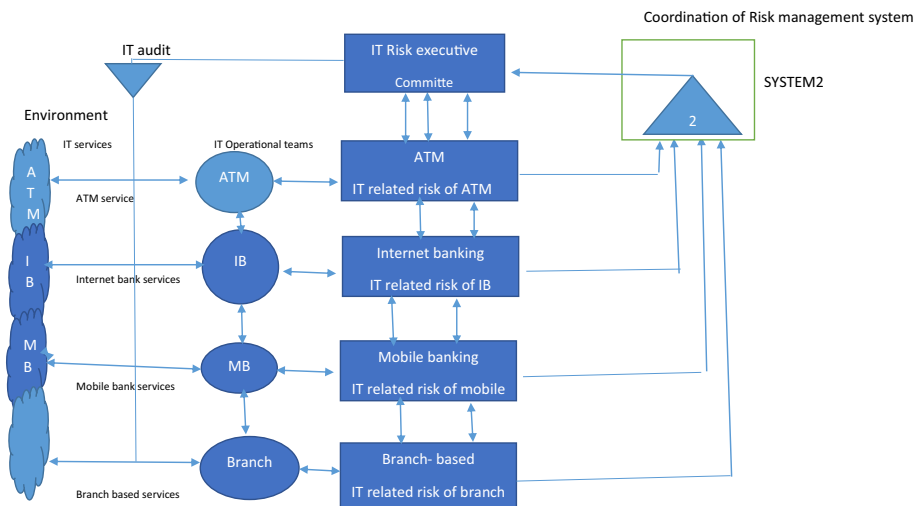


Fig. 8 Design of S2 in e-banking IT related risk

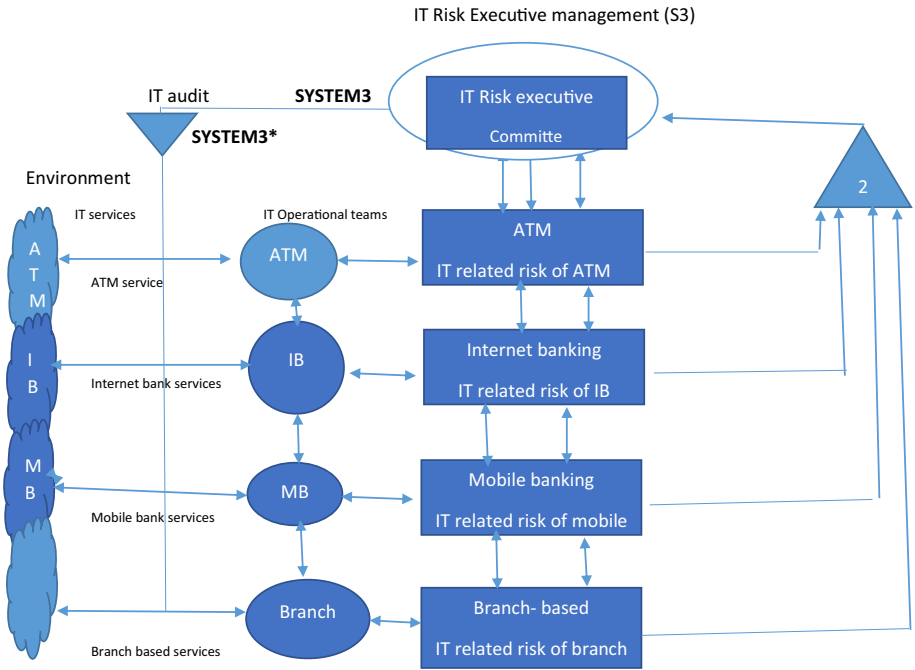


Fig. 9 Designing S3 and S3* (S3)

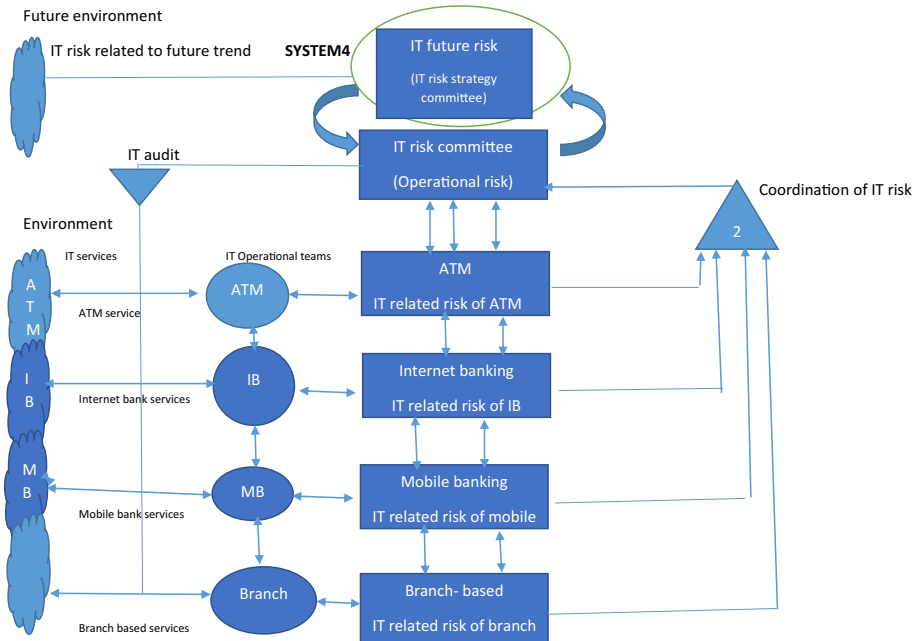


Fig. 10 the IT risk management subsystem S4

Designing S3, S3* (IT Risk Management and IT Risk Audit)

Operational IT risk management (S3) is responsible for the whole IT risk (operations and programs) to ensure the achievement of IT strategic objectives. Managing, controlling, and reporting the operational IT risk (and providing some program and projects for improving the status of IT risks) to the upper level for approving (system 4 and system 5) is the responsibility of this system. Chief Information Risk Officer (CIRO) with the help of the IT operations manager and IT auditor (S3 *) builds the S3 (in some organizations this system can be formed as an IT risk management committee). Figure 9 shows the operational IT risk management system.

Designing S4 (IT Risk Related to Future)

One of the most important components of the VSM is subsystem 4 (intelligence or future management), which is responsible for adapting the organization to the environment according to the trend of future changes. This subsystem ensures the adaptability and viability of the system in the face of environmental dynamic changes. The responsibility of this subsystem is to track the risk related to the future of the IT environment and predict, analyze and simulate the changes and their impacts on the business goals, and if necessary, reconfigure IT risk strategic objectives (by cooperation with S3 which is responsible for current IT risk management and S5 which has the most authority in the system).

In this research, some team member were responsible for analyzing the future trend and evaluates its risks (for example the risks related to cognitive banking or the risk related

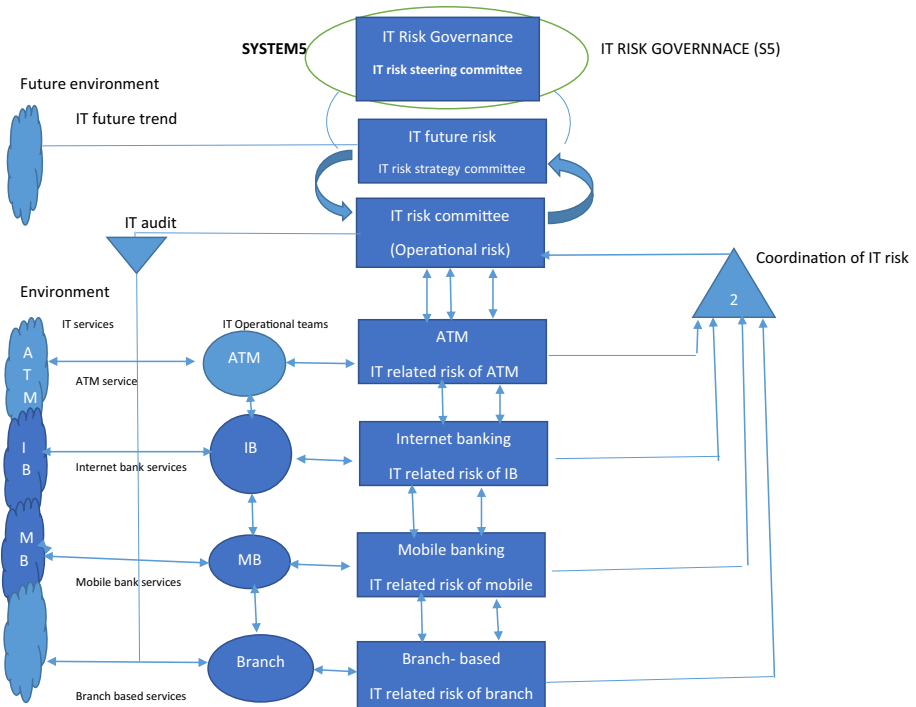




Fig. 11 The Viable IT Risk Management system

to using machine learning technologies in banking context), the future trend of banking services was tracked. The results showed that future trend pointed out that some traditional e-banking services such as old telephone bank services would be replaced by some new and advanced cognitive banking services. Therefore, due to these technological changes, the development of these old services will be limited and some risks related to this service, which was addressed as an important risk in recent years should be reconsidered again. The level of acceptance and threshold risk varied according to a report of future risks. After reconsidering the IT risk strategic plan, some risks accepted and would not invest on in anymore. At the same time, some new risk introduced that requires planning for managing

Table 2 The VSM subsystem of viable IT risk management system

FUNCTION 	Functions
VSM subsystems for IT risk management 	
<p>System 1 (IT risk assessment related to current services) Responsible for managing IT risk related to current services at the front line of the services. Maintaining the current risk profile and reporting At specific intervals is the responsibility of this system (it can be selected from front line employees)</p>	<p>Managing IT risk related to operational services (current IT risk profile)</p> <ul style="list-style-type: none"> - Risk related to ATM services - Risk related to branch services - Risk related to Internet banking service - Risk related to mobile banking services
<p>System 2 (coordination among IT risk activities) Responsible for establishing a shared understanding of IT risk and coordination among different units (S1)</p> <p>Ensuring the continuity of the whole system by coordination among sub system</p>	<p>Providing IT risk standards polices and instructions and communicate to S1</p> <p>Providing IT risk procedure and instructions</p> <p>Providing reporting format for S1</p> <p>Providing training schedules for IT risk</p> <p>Providing meeting schedules among s1 and s3</p>
<p>System 3 (IT risk management)</p> <p>Responsible for managing the whole IT risk operations (current services)</p> <p>Reporting and validating the current IT risk to system 4, 5 (it can be formed as IT risk management committee)</p>	<p>Maintain the current risk profile (Table 3)</p> <p>Assessment of Key Risk Indicator (KRI)</p> <p>Analyzing the effectiveness of the solutions that are used for mitigating risk</p> <p>Analyzing the reports from S4</p> <p>Help to identify a strategic plan for risk with help of S4 and S5</p>
<p>System 3* (IT auditors) responsible for Auditing IT risk teams and report to S3</p>	<p>Audit IT risk in operational units and report to IT risk manager to ensure that risks at operational units are considered correctly</p>
<p>System 4 (risks related to future trend) Responsible for tracking the trend of future changes (business/ IT), analyzing the changes and impacts, Reconfigure IT risk strategic plan to adapt to the enterprise risk management (it can be formed as IT risk strategic committee)</p>	<p>IT risk strategy committee: consists of experts from different IT field to evaluate the future trend of IT risk</p> <p>With the help of system 3, balance the future risk and current risk profile and proposing IT risk strategic plan according to the changes</p>
<p>System 5</p> <p>Responsible for IT risk overall polices, ensuring that IT risk does not exceed the enterprise risk appetite, integrity and alignment between IT risk with Enterprise Risk Management, ensure that the impact of IT risk to enterprise goals is identified and managed (it can be formed as IT risk steering committee)</p>	<p>IT risk steering committee: consists of</p> <p>Member of the board</p> <p>CIO, CIRO, CISO (chief information security officer)</p>

new risk. The changes in the business environment are coming and its risk should be evaluated and introducing to the system for consideration.

Some services will be replaced by new services soon and organizations would not need to invest in the risk of these services (less focus on these risks because of the service retirement). Tracking these changes and reconfigure strategic plans in IT risk is the responsibility of S4. Figure 10 shows subsystem 4 of this research.

Designing S5 (IT Risk Governance)

This subsystem has the most authority in the system (can be formed as IT risk steering committee). One of the responsibilities of this subsystem is defining IT risk overall policies (in line with the enterprise risk policies) and ensuring that IT-related risk does not

Table 3 The summary of IT risk (current profile) that is maintained and managed by S3

	IT risk related to operational services that is Managed by S3 (The full IT risk table consists of the probability, impact, current solution, risk owner...) (most risks related to IT infrastructure are common between all services)
Risk related to hardware and facilities	Risk related to computing and storage capacity Risk related to MTBF of hardware Risk related to redundancy Risk related to maintenance Risk related to physical access Risk related to failure Risk related to power supply, HVAC, ...
Risk related to general software (OS, antivirus, ERP,) and applications (mobile banking, internet banking ...)	Risk related to OS: - Risk related to unpatched vulnerabilities - Risk related to weak control access Risk related to some common software such as ERP and service applications: - Risk related to software bugs - Risk related to updates - Risk related to vulnerabilities
Risk related to Network and Telecom	Risk related to LAN, WAN, telecom Risk related to routing protocol Risk related to capacity of network Risk related to encryption of communication
Risk related to database and data management	Risk related to database architecture Risk related to redundancy of database Risk related to database patch updates Risk related to database backup Risk related to data recovery plan Risk related to data archiving
Risk related to people	Risk related to competency of individual Risk related to knowledge and training Risk related to experience
Risk related to the process of IT operational services	Risk related to the process of maintenance Risk related to process of updating Risk related to process of change management Risk related to process of log management Risk related to incident management
Risk related to suppliers	Risk related to telecom company

exceed the enterprise appetite risk. This system is responsible for evaluating, directing, and monitoring the effective and efficient implementation of IT risk management system in the organization. Establish and maintain a common risk view, integrate with ERM, make risk aware business decision culture are the other responsibility of this system. At the same time, keeping a balance between the current risk status and future IT risk status is the other responsibility if this system. Figure 11 shows the complete practical viable IT governance model based on VSM. Table 2 shows the function of VSM in the IT risk management system. Table 3 shows the summary of the IT risk profile that is maintained and managed by S3.

Conclusion

In this research, by applying the soft system models such as the VSM as an adaptable framework for managing IT risk, we can guarantee the adaptability and viability of the IT risk management system. The VSM has a strong scientific foundation, which based on system science, cybernetics approach, and variety engineering and is a good candidate as a framework for IT risk management system because the dynamic changes of business /IT environment require an adaptable framework for managing IT risks for aligning and integrating IT risk strategy with the business risk strategy.

By using the variety engineering (Ashby law) in VSM, the front line employee is encouraged to manage the IT risk (creating autonomous system 1) and this can be helpful to increase the quality of IT risk management systems by managing risk at the front line (detecting and mitigating risk at the source). The results show us the best approach to manage the IT risk is building an autonomous system (system1) to deal with risk at the front line and VSM brings these benefits for us in system 1. By the communication channels between subsystems in VSM, a big picture of the current IT risk profile shared between the operational units (S1) and the management system and this can be helpful to establish a holistic approach in the IT risk management system. Therefore, the results show us that VSM can propose a holistic approach for IT risk management system, which has not been paying attention to this important point in any other risk framework. Not paying attention to a holistic approach in a risk management system can be a threat of duplicating risk analysis (wasteful work) in different units, which are working in the isolated environment.

The viable IT risk framework uses subsystem 4 (system intelligence) to track and analyze environmental changes and evaluate the future trend of IT risk. Therefore, the results show us (refer to designing S4 section) that by evaluating the future risk of IT and comparing to the current risk profile (which is provided by S3) system 4 can propose a dynamic risk strategy plan that is adaptable to the future trend. Adaptability to future change (in business and IT) has not been addressed by any other IT risk framework.

In recent years, the VSM as a framework applied for IT governance and IT security management system, but this research showed that the VSM could be a good choice for the IT risk management framework.

Despite the many advantages of this system, it also brings some challenges and criticisms. Because VSM is a high-level abstraction of system models, it cannot tell you how you can implement this model in detail by itself and you can use other methodology such as VIPLAN for implementing VSM in your organization. In my opinion, one of the criticism of this model is that, in VSM, system 3 is responsible for stability in the system, and system 4 is responsible for development (change in the system, which is the source

of instability), and maintaining a balance between stability and instability is the responsibility of system 5 but VSM does not pay attention to the details of how these challenges can be solved. In addition, creating an autonomous system (system 1) is a big challenge because we faced a social system in organizations and have to respect and consider all participants in the system but VSM cannot help us in detail how to deal with this challenge. To resolve these challenges, we have to complement VSM with some other approaches such as DevOps and Lean-Agile thinking to help us to solve the challenges. I faced these challenges in my research.

I recommend combining Lean-Agile thinking and DevOps approach (as a suitable approach to improve performance and a good solution for balancing stability and instability dilemma in IT context) and VSM (as a high-level abstraction of an adaptable system model) can be a good choice for future study and research.

Data Availability The datasets generated and analyzed during the current study are not publicly available due the fact that they confidential. However, are available from the corresponding author on reasonable request.

Declarations

Conflict of Interest The author declares that there is no conflict of interest.

References

- Alqurashi E, Wills G, Gilbert L (2013) A viable system model for information security governance: Establishing a baseline of the current information security operations system. Paper presented at the IFIP International Information Security Conference.
- Arghand AA, Alborzi M, Ghatari AR (2021) A methodology for IT governance by viable system modeling (VSM): an action research in designing a data center. *Systemic Practice and Action Research* 1–22
- Beer S (1972) *Brain of the firm: a development in Management cybernetics*: Herder and Herder
- Beer S (1979) *The heart of enterprise (Vol. 2)*: John Wiley & Sons
- Beer S, Beer S (1985) *Diagnosing the system for organizations*. Wiley, Chichester
- Checkland P, Holwell S (1998) Action research: its nature and validity. *Systemic Practice and Action Research* 11(1):9–21
- Coles RS, Moulton R (2003) Operationalizing IT risk management. *Comput Secur* 22(6):487–493
- De Haes S, Van Grembergen W, Joshi A, Huygh T (2020) Enterprise governance of IT, alignment, and value. In *Enterprise Governance of Information Technology* (pp. 1–13): Springer
- De Smet D, Mayer N (2016) Integration of it governance and security risk management: A systematic literature review. Paper presented at the 2016 International Conference on Information Society (i-Society)
- Espejo R, Bowling D, Hoverstadt P (1999) The viable system model and the Viplan software. *Kybernetes*. Hutchinson B, & Warren M (2002). *Information Warfare: using the viable system model as a framework to attack organizations*. *Australasian Journal of Information Systems* 9(2)
- Fazlida MR, Said J (2015) Information security: Risk, governance and implementation setback. *Procedia Economics and Finance* 28:243–248
- Gokhale GB, Banks DA (2004) *Organisational Information Security: A Viable System Perspective*. Paper presented at the AISM
- Goldes S, Schneider R, Schweda CM, Zamani J (2017) Building a viable information security management system. Paper presented at the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF)
- Hutchinson B, Warren M (2002) *Information Warfare: using the viable system model as a framework to attack organisations*. *Australas J Inf Syst*, 9(2)
- Huygh T, De Haes S (2018). Using the viable system model to study IT governance dynamics: evidence from a single case study. Paper presented at the Proceedings of the 51st Hawaii International Conference on System Sciences

Isaca (2009) The risk IT framework: ISACA

Jackson MC (2005) *Systems Thinking: creative holism for managers* 2003. John Wiley & Sons, West Sussex

Lewis E, Millar G (2009) The viable governance model-A theoretical model for the governance of IT. Paper presented at the 2009 42nd Hawaii International Conference on System Sciences

Peppard J (2005) The application of the viable systems model to information technology governance. ICIS 2005 Proceedings 5

Rakers M, Rosenkranz C (2008) Organizational impact on project management in financial data warehousing: a case study

Schwaninger M (2006) Design for viable organizations: The diagnostic power of the viable system model. *Kybernetes: Int J Syst Cybern* 35(7–8):955–966

Schwaninger M, Scheef C (2016) A test of the viable system model: theoretical claim vs empirical evidence. *Cybern Syst* 47(7):544–569

Spyridopoulos T, Maraslis K, Tryfonas T, Oikonomou G, Li S (2014) Managing cyber security risks in industrial control systems with game theory and viable system modelling. Paper presented at the 2014 9th International Conference on System of Systems Engineering (SOSE)

Vahidi A, Aliahmadi A, Teimoury E (2019) Researches status and trends of management cybernetics and viable system model. *Kybernetes*

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.