A COBIT5 Framework for IoT Risk Management

Faride Latifi
Young Researchers and Elite Club,
Damavand Branch, Islamic Azad University,
Tehran, IRAN

Houman Zarrabi
ICT Research Center
Tehran, IRAN

ABSTRACT
Use of information technology management framework plays a major influence on organizational success. This article focuses on the field of Internet of Things (IoT) management. In this study, a number of risks in the field of IoT is investigated, then with review of a number of COBIT5 risk management schemes, some associated strategies, objectives and roles are provided. According to the in-depth studies of this area it is expected that using the best practices of COBIT5 can be very effective, while the use of this standard considerably improve some criteria such as performance, cost and time. Finally, the paper proposes a framework which reflects the best practices and achievements in the field of IoT risk management.

General Terms
IoT, COBIT5, IT

Keywords
IT Management Framework, IoT, COBIT5, Efficiency, Cost

1. INTRODUCTION
The impact and role of information technology is inevitable in any organization, however, management issues and its importance in this area has caused the standard of management and governance frameworks for this purpose have been developed. COBIT5 (Control Objectives for Information and related Technology) is a comprehensive framework that provided for in each area in recent years and is used and helps them to achieve the objectives of governance and management [1, 2, 3].

It should be noted that a standard framework for the assessment of process can be effective in improving the evaluation processes [4].In [5] the impact of information technology on 50 oil companies in Iran is evaluated. In [6] states that the negative effects of risk on the performance of the strategic projects are more. Risks related impact of project management is negative on performance [7]. In [8] the key features that risk assessment should be included in a management information system are discussed. Source [9] has offered a new approach that involves managing financial risks. In [10] a process model depends on the situation with the aim of completing the process of information security risk management is provided. All Organizations providing IT services has strong points that have turned them into a competitive center and weaknesses that need to be improved in the area of performance [11]. In [12] a certain way for the use of risk management based on knowledge provided as a framework to maintain the competitiveness of the business environment. In [13] an integrated and comprehensive approach to information security management is essential for any organization. In [14] a number of best practices are provided that managers need to improve the chances of a successful combination and integration of information technology. This research provides an IoT (Internet of Things) embedded cloud control architecture [17]. This paper lays the foundation for the creation of a safe remote monitoring system for machine tools through IoT devices and analyses the critical issues focusing on the manufacturing environment [18]. In this paper, we present a methodology foundation for analyzing medical contexts. That is, we formalize five representative medical diagnosis schemes for personal healthcare application [19]. This paper will conduct research on the distribution of information security roles and the frequency of such job mobility in order to resolve these problems [20]. The proposed work allows the organization to store the IoT data on the cloud securely by applying different Access control policies and the cryptography concepts [21]. This paper describes an approach based on the exploitation of virtual environments and agent-based simulation for the evaluation of cybersecurity solutions for the next generation of IoT applications in realistic scenarios. The effectiveness of the approach is shown by considering a concrete case study involving the cooperation of real and virtual smart devices inside a virtualized scenario where security issues are first evaluated and then handled [22]. We look into the Smart Parking application domain and provide a solution that protects the privacy of the users by totally avoiding the exchange of confidential information [23]. This article presents five IoT technologies that are essential in the deployment of successful IoT-based products and services and discusses three IoT categories for enterprise applications used to enhance customer value [24]. In this paper, a secure ECC based mutual authentication protocol for secure communication of embedded devices and cloud servers using Hyper Text Transfer Protocol (HTTP) cookies has been proposed [25]. Similar research work in this domain are performed in [25] [26] [27] [28] [29] [30] [31].

2. COBIT5 STANDARD FRAMEWORK
Includes five principles to specific targets in the management and governance of information technology [15]. And is able to evaluate the organizations in achieving their goals. All organizations are able to customize COBIT5 for their different purposes. This IT standard framework covers IT organizational goals end-to-end and is in line with other standards and frameworks. Also included several targets and enabling and distinct them for an integrate governance and management. Its governance Field includes alignment, planning, organization and management processes and management field includes construction, acquisition and implementation, delivery and support services, monitoring, assessment and evaluation processes [15, 16]. In this paper, the framework is used to assess and manage risk.

3. COBIT5 IN FIELD OF IoT RISK MANAGEMENT
IoT as a new vector of bandwidth consumption – Thousands of sensors, or actuators, trying to communicate to a single server will create a flood of data traffic which can easily bring down the server. In Figure 1 some of IoT risks has been shown, that are Data and application, Physical environment, Change management, Third-party supplier and vendors,

Internal employees, Security and Privacy, Infrastructure, Legal and regulatory. Effectively managing IT (Information Technology) risk helps drive better business performance by linking information and technology risk to the achievement of strategic enterprise objectives. Risk is generally defined as the combination of the probability of an event and its consequence. However COBIT5 offers some best practices in this area such as:

- ✓ Understand the drivers, benefits and target audiences from a risk perspective.
- ✓ Understand the components of risk activities.
- ✓ Understand how to use risk scenarios for GEIT.
- ✓ Understand how COBIT 5 for Risk relates to and aligns with other standards.
- ✓ Understand how to use risk scenarios for GEIT.
- ✓ Understand how COBIT 5 for Risk relates to and aligns with other standards.

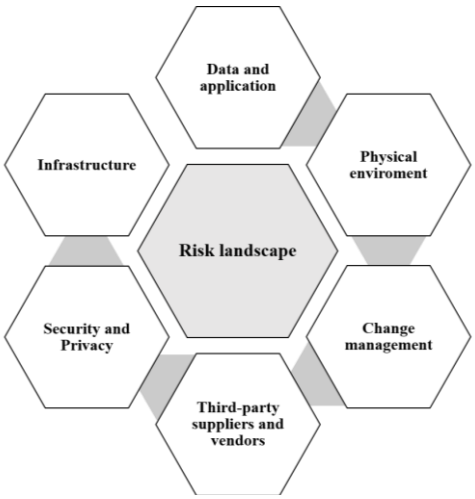

Figure 1: IoT Risks

4. MAPPING THE ROLES AND FUNCTIONS OF COBIT5 WITH IoT RISKS

A general definition of risk means the probability of not being fulfilled predictions. In this paper, risk means the possibility of a damage and financial loss as a result of carrying out an economic activity. Table 1 defines the mapping between the risks taken in the field of IoT. Moreover in the last column of the table some COBIT5 advantages in different areas according to the definition of the roles and functions are listed.

5. THE PROPOSED FRAMEWORK FOR IOT RISK MANAGEMENT

Without a doubt, the standard framework proposed in this paper compared to similar cases in this area is more complete. Because is based on the strongest IT governance and management framework. It should be noted that COBIT5 provides some complete and integrated set of best management practices according to organization's needs. Proposed framework is shown in Figure 2 that is contains of 4 parts, COBIT5 Risk management areas, IoT risks, Roles and operations and impact of this framework on improving a number of qualitative and quantitative criteria.

6. THE PROPOSED FRAMEWORK FOR IoT RISK MANAGEMENT

Without a doubt, the standard framework proposed in this paper compared to similar cases in this area is more complete. Because is based on the strongest IT governance and management framework. It should be noted that COBIT5 provides some complete and integrated set of best management practices according to organization's needs. Proposed framework is shown in Fig 2 that is contains of 4 parts, COBIT5 Risk management areas, IoT risks, Roles and operations and impact of this framework on improving a number of qualitative and quantitative criteria.

7. CONCLUSIONS

COBIT5 strategies in the field of risk management are used widely. In risky areas, organizations usually use the best practices of it. In this article we provided a precise definition of the IoT associated risks as well as a mapping between those risks and the COBIT5 risk management process. The results showed that the use of standard IT management framework can improve a number of quality criteria. Accordingly a framework was proposed for IoT risk management that contains the associate effective processes, roles, operations and risk areas. The favorable effects of its use are reducing the time, costs and increasing the efficiency and productivity.

Table 1: COBIT5 and IoT Alignment

IoT risks	COBIT5 functions	The benefits of using COBIT5
Data and application	Establishes an information life cycle function	Ensuring data are secured and available when and where the business needs them. Ensuring reliability of data Measuring data performance
Physical environment	Implementing physical security measures Selecting and managing facilities	Reducing business interruptions from damage to computer equipment and personnel
Change management	Assessing, prioritizing and authorizing changes	Mitigation of the negative risks
Third-party supplier and vendors	22 mitigation actions	Data loss reduction Decrease in audit findings Cost optimization
Security and Privacy	support the mission of the business and achievement of business goals	Reduced complexity increased cost-effectiveness
Infrastructure	Infrastructure and Applications management	Provide a security architecture Provide security awareness Provide secure development

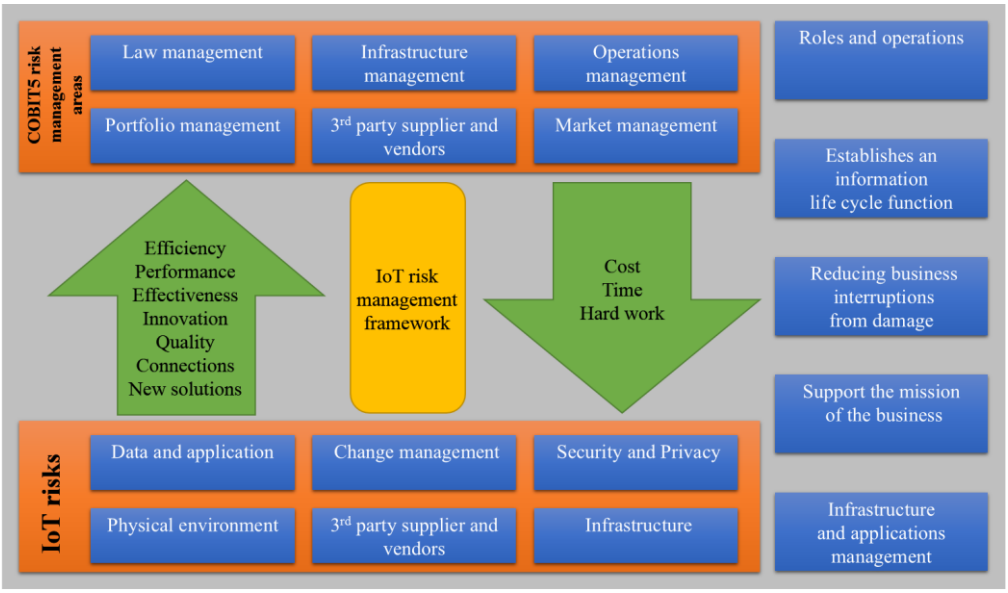

Figure 2: Proposed COBIT5 Framework for IoT Risk Management

8. REFERENCES

[1] The Book of COBIT5: A Business Framework for the Governance and Management of Enterprise IT, available at: http: //www.isaca.org.

[2] Z. Enslin, "Cloud computing adoption: Control objectives for information and related technology (COBIT) – mapped risks and risk mitigating controls", African Journal of Business Management, Volume 6, Sept. 2012, Pages 10185-10194,

[3] COBIT 5, Information Systems Audit and Control Association (ISACA), 2012.

[4] S. Cortina, A. Renault and M. Picard, "TIPA Process Assessments: A Means to Improve Business Value of IT Services", Volume 4, October.2013, Pages 1-18.

[5] Maryam Teymouria, Maryam Ashoorib, "The impact of information technology on risk management", World Conference on Information Technology, Procedia Computer Science, Volume 3, 2011, Pages 1602–1608.

[6] Shan Liua, Lin Wang, "Understanding the impact of risks on performance in internal and outsourced information technology projects: The role of strategic importance", International Journal of Project Management Volume 32, Issue 8, November 2014, Pages 1494–1510.

[7] Shan Liu, "How the user liaison's understanding of development processes moderates the effects of user-related and project management risks on IT project performance", Information & Management Volume 53, Issue 1, January 2016, Pages 122–134.

[8] Alireza Shameli-Sendia, Rouzbeh Aghababaei-Barzegarb, Mohamed Cherietc, ,"Taxonomy of information security risk assessment (ISRA), Computers & Security, Volume 57, March 2016, Pages 14–30.

[9] Sajjad Ahmeda, c, Mohamed Elsholkamia, Ali Elkamela, Juan Dub, Erik B. Ydstieb, Peter L. Douglasa" Financial risk management for new technology integration in energy planning under uncertainty", Applied Energy Volume 128, 1 September 2014, Pages 75–81.

[10] Jeb Webb, Atif Ahmad, Sean B. Maynard, , Graeme Shanks, "A situation awareness model for information security risk management", Computers & Security Volume 44, July 2014, Pages 1–15.

[11] Benjamin B.M. Shaoa, Winston T. Linb, "Assessing output performance of information technology service industries: Productivity, innovation and catch-up", International Journal of Production Economics Volume 172, February 2016, Pages 43–53.

[12] Samer Alhawaria, , Louay Karadshehb, , Amine Nehari Taletc, , , Ebrahim Mansoura, ," Knowledge-Based Risk Management framework for Information Technology project", International Journal of Information Management, Volume 32, Issue 1, February 2012, Pages 50–65, Volume 34, Issue 1, January 2016, Pages 102–116.

[13] Zahoor Ahmed Soomro, Mahmood Hussain Shah, Javed Ahmed", Information security management needs more holistic approach: A literature review", International Journal of Information Management Volume 36, Issue 2, April 2016, Pages 215–225.

[14] Franz T. Lohrkea, , Cynthia Frownfelter-Lohrkea, , David J. Ketchen Jr.b"The role of information technology systems in the performance of mergers and acquisitions", Business Horizons, Volume 59, Issue 1, January–February 2016, Pages 7–12.

[15] The Book of COBIT5: A Business Framework for the Governance and Management of Enterprise IT, available at: http: //www.isaca.org, 2016.

[16] COBIT 5, Information Systems Audit and Control Association (ISACA), 2012.

[17] Hyunsoo Lee, "Framework and development of fault detection classification using IoT device and cloud environment", Journal of Manufacturing Systems, Volume 43, Part 2, April 2017, Pages 257–270.

[18] Stefano Tedeschi, Jörn Mehnen , Nikolaos Tapoglou , Rajkumar Roy, "Secure IoT Devices for the Maintenance of Machine Tools", Procedia CIRP, Volume 59, 2017, Pages 150–155.

[19] Hyun Jung La, "A conceptual framework for trajectory-based medical analytics ", Journal of Computer and System Sciences, Volume 82, Issue 4, June 2016, Pages 610–626.

[20] Sangho Park, Yanghoon Kim, Hangbae Chang, "An empirical study on security expert ecosystem in the future IoT service environment", Computers & Electrical Engineering, Volume 52, May 2016, Pages 199–207.

[21] Jayant D. Bokefode, Avdhut S. Bhise, Prajakta A. Satarkar, Dattatray G. Modani, "Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption", Procedia Computer Science, Volume 89, 2016, Pages 43-50.

[22] Angelo Furfaro, Luciano Argento, Andrea Parise, Antonio Piccolo, "Using virtual environments for the assessment of cybersecurity issues in IoT scenarios", Simulation Modelling Practice and Theory, Volume 73, April 2017, Pages 43–54.

[23] Ioannis Chatzigiannakis, Andrea Vitaletti, Apostolos Pyrgelis, "A privacy-preserving smart parking system using an IoT elliptic curve based security platform", Computer Communications, Volumes 89–90, 1 September 2016, Pages 165–177.

[24] In Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises", Business Horizons, Volume 58, Issue 4, July–August 2015.

[25] Sheetal Kalra, Sandeep K. Sood, "Secure authentication scheme for IoT and cloud servers", Pervasive and Mobile Computing, Volume 24, December 2015, Pages 210–223.

[26] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi, "Internet of Things security: A survey", Journal of Network and Computer Applications, Volume 88, 15 June 2017, Pages 10–28.

[27] Mohammad Amin Hatef, Vahid Shaker, Mohammad Reza Jabbarpour, Jason J. Jung and Houman Zarrabi, "HIDCC: A Hybrid Intrusion Detection Approach in Cloud Computing", Concurrency and Computation, Wiley, 2017. (To Appear)

[28] Reza Omidi, Houman Zarrabi, "New Protection Technique Against Unidirectional MEUs for FIR Filters", Springer Science+Business Media New York, 31 March 2017.

[29] Armin Nabaei, Melika Hamian, Mohammad Reza Parsaei, Reza Safdari, Taha Samad-Soltani, Houman Zarrabi, A. Ghassemi, "Topologies and performance of intelligent algorithms: a comprehensive review", Springer Science+Business Media Dordrecht 2016.

[30] Amin Mohajer, Morteza Barari & Houman Zarrabi, "Big Data based Self-Optimization Networking: A Novel Approach Beyond Cognition", Intelligent Automation & Soft Computing, 2017.

[31] Mohammad Emamil, Mohammad Reza Jabbarpour, Bahman Abolhassani, JasonJ.Jung, Houman Zarrabi, "Soft Cooperative Spectrum Sensing using Quantization Method in the Presence of Smart PUE Attack", Springer Science+Business Media New York 2017.