Agile Approach with Kanban in Information Security Risk Management

Vasile Dorca, Eng. Phd. Stud.
Electrical Engineering
Technical University of Cluj-Napoca, UTCN
Cluj-Napoca, Romania
vdorca@live.com

Sorin Popescu, PhD. Eng. Prof.
Design Engineering and Robotics
Technical University of Cluj-Napoca, UTCN
Cluj-Napoca, Romania

Radu Munteanu Jr, PhD, Eng. Assoc. Prof.
Electrical Engineering
Technical University of Cluj-Napoca, UTCN
Cluj-Napoca, Romania

Adrian Chioreanu, PhD, Eng.
Electronics and Telecommunications
Technical University of Cluj-Napoca, UTCN
Cluj-Napoca, Romania

Claudius Peleskei, Eng. Phd.Stud..
Electrical Engineering
Technical University of Cluj-Napoca, UTCN
Cluj-Napoca, Romania

Abstract:
In an ever changing business environment, in order to bring value, security risk management must keep engaged at pace with the company, by following the enterprise goals and using the same methodologies as core business units. This paper analyses how information security risk management can be automated and interlinked with the processes in a software development company, using an Agile approach with Kanban. The methodology used has been tested (Proof of Concept) applying relevant information security risks for an e-commerce business, the results showing an increase in efficiency of the risk management team, better business response and improvements of the defined risk management SLAs (Service Level Agreement).

Keywords – *information security risk management, Agile, Kanban*

I. BACKGROUND

A. Information Security Risk management

The background of the paper is intended to clarify the state of the art and current situation based on existing studies and literature.

All organizations are exposed to information security risk impacting the organization in a different manner and with a different magnitude [1]. Risk is a function of the likelihood of a given threat exploiting a potential vulnerability, which results in an impact of that event on the organization. The scarcity of resources and the changing nature of the threats and vulnerabilities landscape make completely mitigating all risks impractical [8].

Risk management offers a toolset to assist the organization in sharing a commonly understood view with IT and business managers concerning the potential impact of various IT security related threats. The risk management function must help the organization to understand and make informed decisions to mitigate the risk or pursue the most appropriate course of action [9].

B. Information Security Risk Management challenges

In every enterprise, information security risks can be found across all departments, meaning that the department owners are accountable for the risks within their area. The security team is responsible to support and provide expertise to the business owners to take the right decisions and to mitigate the risks they face. Both parties, security professionals and key business players (department owners) of the information security risk management lose from sight risk management related tasks or fail to accomplish tasks within the SLA due to having separate backlogs (tools) for their daily work and risk management [10].

Making a short research, we realize that the majority of the risk management methodologies (e.g. COBIT for Risk, Gartner Risk Management) don't provide details on tools to be used in managing risks within the enterprise, or they provide specific Risk Management tools that are not in line with the working approach that companies have, so risk management ends up being a separate process, using different tools/work trackers than the enterprise, creating sometimes big challenges in treating risks. Conducting surveys with different security professionals and development managers proved us that often risk management related tasks (e.g. assessment, monitoring, or mitigations) are difficult to get prioritized against the tasks already agreed in daily scrums using the Kanban board. At time the information security team in general and the risk management team in particular may be overloaded with tasks

that they need to tackle based on business strategy, goals and priorities.

Risk teams usually have multiple responsibilities and perform various activities [11], some of them with a predictable nature (e.g. reporting) some with an ad-hoc nature (e.g. risks identification). Tasks that are to be performed by the risk team are gathered in different buckets of work from different streams within the business. The risk function must offer a consistent and predictable, yet flexible way of tackling work, prioritizing it in order to maximize resources and help attain business goals.

As the threat landscape is increasing in diversity and enterprises are embarking in new endeavors, the information security team must be able to identify and manage new risks on a daily basis [12]. One of our main concerns as a risk team is that ad-hoc work, such as risk identification and risk assessment interferes with our daily activities such as reporting, planned assessments, training.

C. Agile methodology

The Agile manifesto [2] states that "we have come to value through:

- Individuals and interactions over processes and tools;
- Working software over comprehensive documentation;
- Customer collaboration over contract negotiation;
- Responding to change over following a plan."

The Agile philosophy is strongly influenced by product manufacturing concepts such as "Lean Manufacturing" and "Lean Engineering" all of them having birth in the Toyota Production System [13]. Agile it's about empowering the teams to self-manage and it's geared towards avoiding unnecessary activities and reducing burdens on teams and the same time offer a flexible framework to cope with unexpected changes and requirements. Agile techniques, be them SCRUM, Kanban, XP, RAD, Spiral, are very popular in software development companies. Agile is meant to improve the output by improving the flow and streamline the activities.

D. Kanban

Depending on the actual type of work, some Agile methodologies are more suited to some teams, some to others, e.g. SCRUM is typically used by development teams working in sprints [14], whereas Kanban [15] is often used by service or support teams that are not delivering work in sprints.

As information security (risk management in particular) is a service providing team, Kanban is the most suitable Agile model. There are a few particularities that define Kanban: Uses Kanban board with cards for visualization of work/tasks; Tasks have priorities and stages; It's a Pull system, where late process stages pull items from earlier process stages; Problems move forwards, never backwards.

II. HOW WE APPLY KANBAN

A. Motivation, Idea and Vision

The goal is to make the risk management function work within SLAs and at the same time to be able to cope with an increased stream of work. In order to cope with the increased stream of work we needed to eliminate redundant or unnecessary activities (reduce waste) and to create the means to be able to register, track and deliver more tasks (increase throughput and output), thus we needed to be leaner.

Alan Morgan has remarked in his "Agile Risk Management" book [3] that in order to expand the progress and "embrace change", Agile risk management should encourage practitioners to "embrace risk". The Agile risk management has three main principles:

> *"• **Transparency:** Make visible and accessible all risk artefacts…*
>
> *• **Balance:** Establish clarity…*
>
> *• **Flow:** Ensure that risks do not inhibit the project…"– Alan Moran – Agile Risk Management.*

B. Use of Kanban in the daily Operational Security Risk Management;

The security risk management process covers all the security risks across the enterprise regardless of the business areas (i.e. Technology, IT, Finance, HR, etc.), meaning that the business owners are accountable for the risks within their areas. The process itself it's generally governed by the Information Security team. These cross-functional dependencies create challenges on both sides (business and security) due to different priorities, unplanned requirements that are coming from multiple areas and due to a variety of tools used to track the work backlog. This paper aims to overcome these challenges and try to integrate the risk management process that uses different tools in the business daily operations that adopts an Agile approach using Kanban. Beneficial to this scope's accomplishment, three main objectives have been set:

1. Conduct a focus group to define and connect the risk management tasks resulted from the process itself with the Kanban board (including the definition of the RM roles);
2. Propose methods to support the joint of two processes and identify an interconnection module between the risk management tasks and the Kanban board;
3. Measure the outcome results;

In order to achieve this, a first analysis has been made to link the risk management functions overseen by the security risk team with the Kanban board that the business uses to track the backlog of work. The framework used for the risk management and governance is based on COBIT for Risk [16] and the tool used is a service management tool named Service Now.

Based on "COBIT 5 for Risk" framework we're seeing a risk as being in one of the following states in its lifecycle: Identification, Draft, Assessment, Documentation, Acceptance, Treatment, Closure, which are all linked to the three domains defined for the Risk Governance, namely: Monitoring, Prioritization and Exposure Management, Fig. 1. Jake Kouns and Daniel Minoli in their book "Information Technology Risk Management" [4], emphasize the fact that defining roles and responsibilities is a key factor in the success of the risk management process. Conducting a focus group formed by experts in information security field and authors of this article, five roles have been defined as being key in the process: Risk Identifier, Risk Team (formed by experts in the Risk Management field), Risk Owner (the appropriate individual who is the most impacted if the risk gets materialised), Treatment Owner (the individual who is

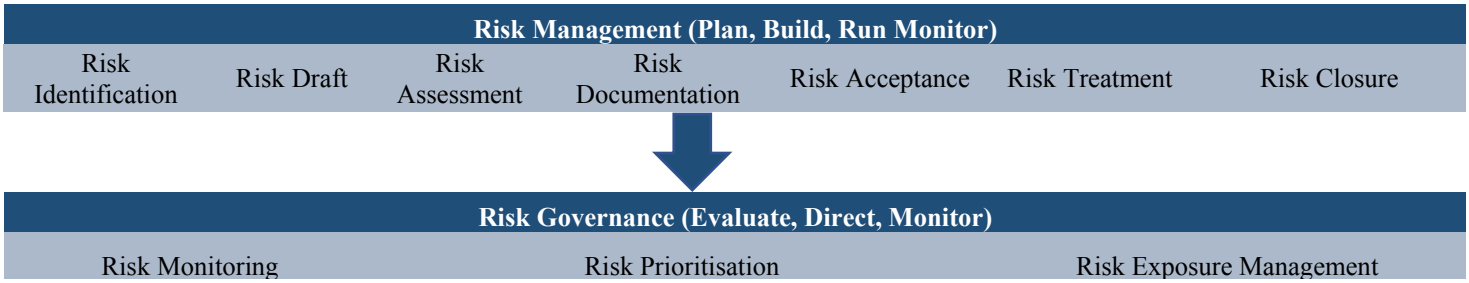

Fig. 1. Risk Management and Risk Governance

responsible for implementing the treatment plan according to the risk owner decision), Security SME (the individual part of the information security team who provides expertise and support in risk context). The risk raiser can be and is encouraged to be anyone in the company who raises risks that is aware of. Given that usually the risks are raised by the risk team or the security SME and the risk identifier responsibility ends actually in the first phase of the process, the focus group has decided to exclude the risk identifier role from this analysis. Table 1 shows the key tasks resulted from the risk management and governance process that should be created in Kanban for each of the roles involved in the risk process starting from identification of a risk until closure. The created tasks will support getting the risk to be progressed, tasks visible and assigned into the business ways of working.

TABLE 1. RISK ROLES AND RESPONSIBILITIES

		Risk Management Roles			
		Risk Team	**Risk Owner**	**Treatment Owner**	**Security SME**
Risk Management Stages	**Risk Identification** (The risk gets identified)				
	Risk Draft (Risk is drafted by the raiser)				
	Risk Assessment (Risk is reviewed, agreed and completed by the RM team)	**Kanban Task** Reviews and confirms the content of the risk, rating and methodology			**Kanban Task** Finds and documents the risk, proposes recommendations and treatment decisions, defines the risk owner
	Risk Documented (RO - gets notified about the risk)		**Kanban Task** Reviews, proposes treatment decisions, and decides treatment and action owner. Decides about the target risk rating		
	Risk Acceptance (Risk gets accepted based on the cost/benefit analysis)	**Kanban Task** To review the authority of the acceptance			
	Risk Treatment (The plan is defined to treat the risk)		**Kanban Task** Asigns a treatment owner	**Kanban Task** Takes action on the risk treatment decision	**Kanban Task** Provides support, advice and consultancy
	Risk Closure (Treatment plan delivered, evidence collection)		**Kanban Task** Submits the risk for closure		**Kanban Task** Ensures the current risk rating is in accordance with the target risk rating
Risk Governance	**Risk Monitoring** (To keep the momentum going, the risk is periodically evaluated and monitored)	**Kanban Task** Provide regular reports on to the Risk owner on all relevant risks		**Kanban Task** Provide regular update on progress against the treatment plan	
	Risks prioritization (Based on the business needs and management feedback, the risks get prioritized)	**Kanban Task** Weekly reviews of all risks to prioritise the work			
	Risk Exposure Measurement (The risk exposure of the enterprise to be constantly measured and input delivered to the business)	**Kanban Task** Risk Committee reviews of metrics and KPI's			

By using a different methodology, the above analysis has confirmed the criticality of risks ownership (included in the daily operations) defined in roles and responsibilities to all enterprise actors in reducing the risk exposure within the organization. The conclusion is also confirmed by ISACA in "Transforming Cyber Security" book, in 2010 [17]. While security tasks are key to be done at the beginning of the process to ensure the risk is well structured, assessed and documented, the owners of the risk have responsibilities around risk treatment, decisions and progress. Even if at first sight the treatment owners seem to have less tasks assigned in the Kanban board, their role is crucial in implementing the risk treatment agreed by the risk owner and resulting in the risk reduction, which is the most impacted objective of the entire risk management process.

At this stage, we can say that now there is a clear view around tasks that should be created and assigned in Kanban for each of the roles in reference to the risk management process that is handled in Service Now. This helps the business to have constant visibility on the tasks they need to perform on risks in their ownership on one hand and it helps the risk management team to address the tasks using a single communication way directly in the Kanban board. This practice of assigning tasks by the risk team in Kanban to all the roles has been applied and observed by a team of experts in a private company for a period of time. While we could observe a better level of engagement from the business into approaching and prioritizing the risk management tasks, the workload of the risk management team has not decrease, as all the tasks have been created manually, so the next step is to create a way to automate this process by developing a module that links the two systems: 1. the service management tool used for risk management and 2. agile Kanban used by the business.

The image below, Fig. 2, shows the correlation created between the two systems and details the initiation of the Kanban assignments resulted from the different risk stages and the linkage between them. Generally the Kanban board contains multiple tasks, from a variety of sources, one of them being the risk management process (see detailed below). Each of the assigned task has a marked color (on the top-left) in accordance with the criticality of the risk in scope: Red for High and Critical, Blue for Medium and Green for Low and Very Low risks. The color code scope is to support the risk roles in having another method of prioritizing their tasks. The tasks are usually assigned into the backlog column and each of the roles are able to decide the preference to resolve the task, the exceptions being the Critical and High risks that are automatically allocated to the "In Progress" column, meaning the task must be dealt with as soon as possible.

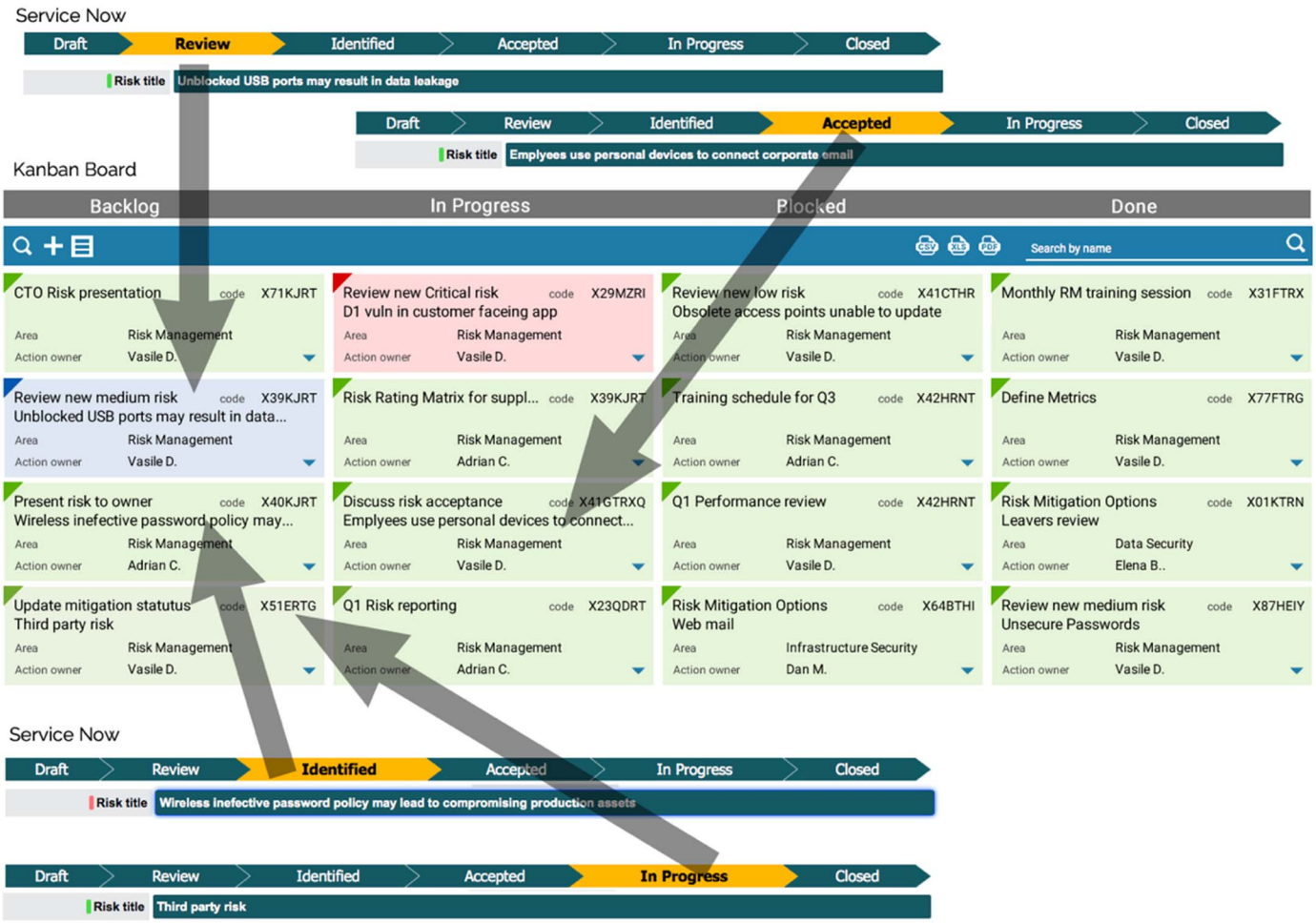

Fig. 2. Status of risks in the Risk governance software and tasks created on the Kanban board

Kanban based on criticality: GOVERNANCE

Risks are being tracked based on criticality, namely Critical risks are being followed by the Security SME on a monthly basis, High risks every three months and Moderate risks every 6 months. Taking into account the criticality, a Kanban ticket is being created for the Security SME every six, three or one month to follow the risk status and updates. This reduces the overhead for the Security SME to track risk updates timeframes. The ticket is being inserted in the Backlog for the appropriate Security SME and is being highlighted in red if the risk is in the top 10 risks list.

Once the correlation between the Risk Management process and the Kanban board has been defined and agreed with all the relevant parties in the business, the focus group have started to measure the progress of the risks already identified in the risk register of a private company (Senior Security Consulting). The evolution in time and the results of the risks monitoring are described in the following image. There were two metrics considered relevant to take conclusions and measure the efficiency of this methodology: the progress of the risks in correlation with a) the breached SLA's of the risk management process (SLA Slippage in terms of days) and b) the response decisions on the identified risks (Identified to Decision in terms of days).

On the OX axis, the focus group has pointed out the major milestones of the monitored evolution, to better understand the trends of this progress and the efficiency of the methodology, so the key milestones are: Risks Collected, Introduction of Roles, Risk Management tool, Risk Management process integration into Kanban (RM & Kanban).

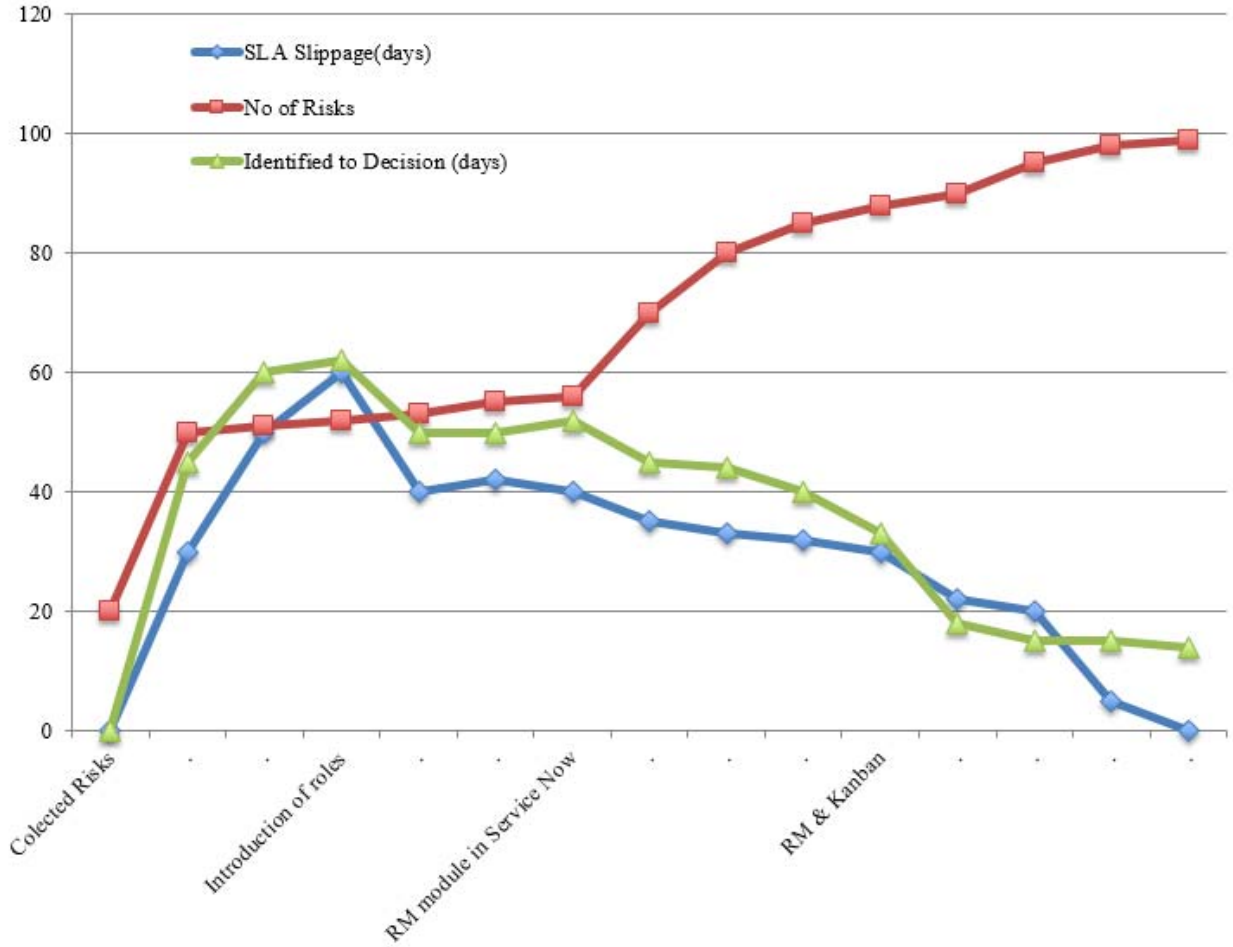

Fig. 3. Trends on Risk governance performance tracked against risk management process changes over time

In Fig. 3, the graph trend shows that while the number of identified risks increased over time, due to the usual risk identification process which is meant to organize workshops to identify new risks, the SLA slippage and "Identified to Decision" started to decrease after the Risk Management tool has been introduced. The figure was compiled based on the evolution over time of a company's risk register. The correlation of the RM tool and Kanban proves to have success in improving the efficiency of the risk management process and in involving the risk players much more in the risk process.

III. CONCLUSIONS

The main contribution described in the paper is the use of Kanban for the Risk Management process and the study on the risk exposure outcomes over time when using this methodology. By adopting the methodology described in this paper, the Risk Management process was directly integrated in the development pipeline, thus tasks raised by the Risk Management process is now on the same backlog with the development stories. This allows a better prioritization of tasks for the Risks Management related tasks for both development teams, business and security. By using a single backlog it is easier to track and forecast the effort needed for tasks related

to security in general and to risk management in particular, thus time and effort for risk management may be budgeted as early as for any other tasks. Using the above approach the Governance of the Security Risk Management process was automatized, resulting in it being more effective and efficient for the business.

IV. REFERENCES

[1] Steve Elky, An Introduction in Information Systems Risk Management, May 31, 2006 - SANS

[2] Multiple authors, Manifesto for Agile Software Development, 2001 http://agilemanifesto.org

[3] Dr. Alan Moran – Agile Risk Management, Springer Briefs in Computer Science, 2014

[4] Jake Kouns and Daniel Minoli - "Information Technology Risk Management", 2010

[5] Betfair, 2015 – Security Risk Management

[6] Senior Security Consulting, 2012

[7] ISACA Risk Management, 2016

[8] Pa, N.C., Anthony Junior, B.; A model of mitigating risk for IT organisations; Aug 2015, Software Engineering and Computer Systems (ICSECS), 2015 4th International Conference on Software Engineering and Computer Systems (ICSECS)

[9] Robert S. Kaplan, Anette Mikes; Managing Risks: A New Framework; June 2012, Harvard Business Review

[10] W. Flores, M. Ekstedt; Exploring the Link Between Behavioural Information Security Governance and Employee Information Security Awareness; (HAISA 2015), Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance

[11] Gary Locke, Patrick D. Gallagher; Managing Information Security Risk Organization, Mission, and Information System View; March 2011, NIST Special Publication 800-39

[12] McAfee Labs Threats Report: August 2015; online http://www.mcafee.com/mx/resources/reports/rp-quarterly-threats-aug-2015.pdf

[13] P. Middleton and J. Sutton, Lean Software Strategies. New York: Productivity Press, 2005.

[14] Linda Rising and Norman S. Janoff; July 2000; The Scrum Software Development Process for Small Teams; IEEE Software archive, Volume 17 Issue 4, July 2000, Page 26-32

[15] Nilay Oza, Fabian Fagerholm, Jürgen Münch; How Does Kanban Impact Communication and Collaboration in Software Engineering Teams?; Proceedings IEEE CHASE 2013, San Francisco, CA, USA; page 124-128

[16] COBIT 5 for Risk, http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx, 2015

[17] ISACA, Transforming Cybersecurity, 2010, online ISACA