Incorporating Information Security into IT Project Management (A Proposed Framework)

Sahira Sangi[1], Mustafa Ilkan[2], Hakan Tokgöz[3]

School of Computing and Technology, Eastern Mediterranean University, Cyprus

Abstract: *The study mainly focuses on the importance of information security and its integration with IT project management in form of a framework. The purpose to design this framework is to provide IT project managers a clear picture of security controls to be adopted in each phase of project management. The study is based on previous synthesis in this domain that supports the aim of this study. The designed framework is basically a combination of IT project management, system development life cycle and essential information security controls. This is a general proposal and need to be implemented practically in further researches to analyze its effectiveness.*

Keywords: *IT security, IT Project management, Information security integration into IT project management*

1. Introduction

IT firms relies upon project management approach to successfully accomplish their projects and without IT security an IT Project cannot be considered as a complete project. Michelle Pruitt (Program Analyst at U.S. Department of Veterans Affairs) stated that project-based firms usually depend on system developers and project managers to ensure the security aspects of concerned project. IT projects developed for government or any national entity has an extra burden over project managers of staying updated with new security necessities. Humans are the primary source and the weakest link of IT projects [1]. This statement actually points to the importance of having human resource equipped with security knowledge and skills. The distinction between project success and failure is the adoption of security best practices. IT project managers are obligated to initiate, execute, monitor and audit the processes. An old famous quote is "what's worth doing is worth protecting" can be related to the security need for an IT project. Where, there is no security, there are significant chances of IT project failures. Therefore, a project manager should make his team members to ensure the security of a project at every phase by creating awareness of security importance for project success. Hence, in communication planning, security should be an input [2]. Therefore, the main idea behind presenting this combine framework is to provide one direction to project managers to complete IT projects successfully. It is a proposed framework, designed with the help of existing theories of various security experts and security firms. Qualitative research approach is been adopted in order to achieve study goals [3].

2. Literature Review

This section first presents the different survey that covers major causes of IT project's failure and secondly, researchers' point of view on security importance to accomplish successful IT projects.

2.1 The Biggest Project Failures

Goatham specified in his survey [**4**] "the story behind the High Failure Rates in the IT Sector" that IT industry has higher rates of project failures over the last years than other industries. According to him the most significant reasons of failure were poor planning and performance. While, private organizations have shown better results. 43% of 400 respondents agreed recent project failures in a survey done by Information Systems Audit and Control Association. A Gartner user survey shows that the large IT projects have a larger ratio of project failures than small ones. He concluded in his survey that most of the reasons of all failures of the projects were: poor quality, high cost, unmatched deadlines, bad decision making and poor functionality. He demonstrated the result by project size [**5**]. The International Business Machines (IBM) research, conducted in 2012, illustrates that only 40% of projects meet schedule, budget and quality goals

and the rest fail. Research indicates the people as the biggest factor or barrier of project success. The analysis of the research showed that between 65 and 80% of IT projects couldn't meet their objectives, time or predefined budget." One Canadian study stated that: Lack of communication between the parties is the cause of IT project failures in 57% of cases they studied [**6**]". An industry research revealed that in comparison to small IT projects, large IT projects have high chances of failures. Larger IT projects with more than $15 million budget mostly fail and increase bankruptcy chances for the company [**7**]. Sainsbury's, the big British supermarket decided to buy a system in order to increase competence and modernize operations of its services. After the system purchased and installed successfully, few days' later system start generating barcode reading errors. Nevertheless, project managers claimed that the system was developed properly. However, within 2 years entire project went off and Sainsbury bears $265,355 million loss in IT costs [**8**].

2.2 IT Projects, Management & Security

IT project management is a technique to build a complex data center, a custom application, or any new information system [**9**]. Security should be planned and maintained at each level of project instead of looking at the last. This approach does not only design strong security architecture but it is also very cost effective. Value of security should be determined before initiating any project. It is considered as a major part of cost & quality of a project that comprises costs such as preventive cost and the cost of failure to create a quality product. Security measures require capital and project managers generally make analysis before investing in security [**1**]. The de-facto standard of project management PMBOK (Project management body of knowledge) is highly adopted by project managers to manage a project. It is almost equally applicable for various kinds of projects such as: home construction, system development or any scientific project. The PMBOK addresses all the areas of project management except security, this is where it fails [**2**]. Dan Emory, a Senior Security Engineer at NetSec, stated that the concept of secure project management merges project management and security needs together. His study proved that the project security should not be taken as system security. When it comes to the security of project management, it must cover the CIA (Confidentiality, Integrity & Availability - the triple constraints of security). Project information protection, authenticity and timely accessibility are essential to reduce the possible project risks. The project information can comprise of cost, scope, agreement information, staffing, communication channels, and procurement, etc. Different organizations might have different information classification and their needs of security [**3**]. The rapid growth in the use of technology and the increase in connectivity between network environment and information systems have increased the chances of vulnerabilities and threats. Hence, it is essential for organizations have competent information security programs. Thousands of organizations around the globe are adopting and implementing security standards based on security best practices to manage their information systems. Compliance with these security standards ensures that the organizations' information is secured competently and also helps in reducing project failure chances [**10**].

3. Security Essentials for IT Project Managers

As shown in various authors' reviews and researches in the previous section, the major causes of IT projects' failures include poor planning, management, improper risk analysis, lack of resources, miss-communication, and others. Previous studies refer that by including security best practices in every phase of a project, IT project managers have the opportunity to deliver more secure systems in a more secure manner. Thus, this section presents security essentials for IT project managers:

3.1 CIA Triads

IT projects are always sensitive to data confidentiality, whether they offer a new technology or existing one because they contain enormous knowledge of network and system architecture. Maintenance of CIA triads not only ensures the availability and integrity of data, but also strengthens the credibility and dividend of companies who really cares about it [**2**].

3.2 Security Program
In the first phase of the initiation security program that consists of policies, standards and guidelines should be developed. Policy is a high level document that defines project objectives and standards that ensure compliance of policies and guidelines help to achieve those objectives. The most common standard used to achieve successful security program is ISO 17799. This standard actually has two parts: BS7799 Part 1, which outlines control objectives and a range of controls that can be used to meet those objectives; and BS7799 Part 2, which outlines how a security program can be set up and maintained [**11**].

3.3 Risk Management
In 2003, a white paper got published by SANS, in which Jeff Christianson stated that "security value can only be truly justified when the risk is fully managed against the overall project cost and its maintenance" [**12**]. Thus, an effective Risk management is considered as a basis of secure project. A security risk is always expected for an IT project and this estimation covers four key areas: data type, breach cause, evidence of misuse and the size of the incident [**2**].

3.4 Team Development
Developing teams and hiring the right people is a challenging task for IT project managers because a poorly developed team can sabotage an effective project plan. In order to accomplish project goals successfully, IT project manager needs to have planning team, risk management team, security experts, system analysis and design team, system and network administrators, incident handling team, penetration testers, auditing team [**13**].

3.4.1 Security Awareness
Security should be considered right from the beginning of the IT project to avoid all possible chances of project failure. As, human resource is the crucial and the weakest link of security, thus, it is necessary for IT manager to create security awareness among team members to realize them that why security is necessary for project success [**14**].

3.5 Access Management
Access management refers to the project member's access to the information, but also system, premises and any project asset. In order to securely manage projects, IT project manager needs to implement, identification, authentication, authorization and accountability policy for all project members. Access control management can be achieved in following terms [**15**].

3.6 Security Architecture & Design
Whether an operating system, an application, or a database is going to be developed, its architecture should be based on security. It requires meeting various security standards and one of them is the TCSEC that evaluates a system or application design against security requirements. For example, an application must be coded securely [**17**].

3.7 Business Continuity and Disaster Recovery
As we have seen in studies, most of the projects failed due to political interruption and environmental circumstances. Thus, in order to keep running the project in every situation, IT project manager should also develop a business continuity plan [**18**]. In case of disaster, there should be a team who can recover business quickly, while other members can keep continue the necessary operations. This can be achieved by performing a business impact analysis, identifying resource values and determining project priorities and incident or crisis management plans [**17**].

3.8 Secure Documentation
A formal and secure document should be prepared to record all security requirements for the project. This document usually named as security management program (SMP) document. These documented requirements can be used later on as a reference for further project tasks. This SMP is normally a comprehension of all used plans such as risk management, work breakdown structure, assigned roles and

responsibilities, project charter, scope and secure communication requirements, etc. The SMP also contains designed security policies, standards, procedures, regulations and guidelines [**2**].

3.9 Penetration Testing

To evaluate how vulnerable a newly or existing system is and what impact it can cause on the entire project in case of exploitation, the penetration must be performed. To ensure the effectiveness of applied security controls, only unit testing is not enough IT project manager must get done penetration testing. Security can never be guaranteed until penetration testing is performed [**19**].

4. System Development Life Cycle Security & IT Project Management Models

System development is also a main concern of IT managers, but the nature of the system could be different. Thus this section presents existing models of SDLC with IS (Information System) and ITPM (Information Technology Project Management) with SDLC (System Development Life Cycle).

4.1 SDLC Integrated with Security

According to NIST "Security assurance at each level of system development reduces risk of project failure and save all information assets of the project. The development lifecycle is a process that initiates with the development of a new project and ends with the disposal of the previously developed system or application [**20**]. The Figure 1 below shows how security can be incorporated into each phase of the SDLC:

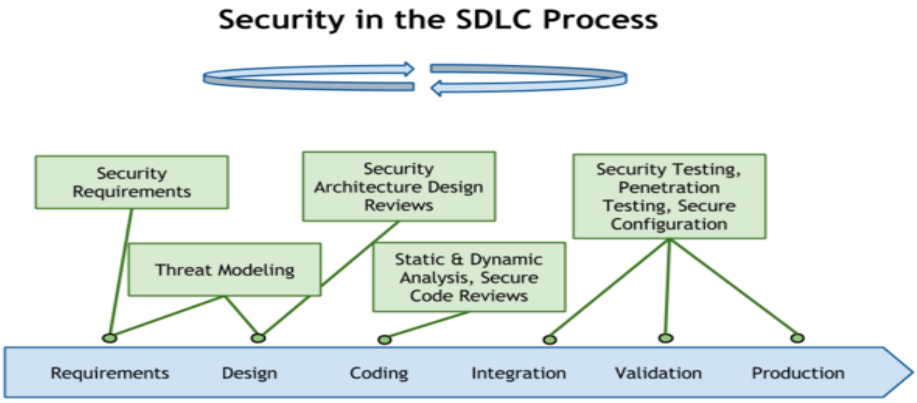

Fig. 1: Security integration in SDLC

In order to develop a secure system, each phase of system development lifecycle comprises following security requirements [**21**]:

- **Initiation:** Security program requirements and security impact on cost & benefit of the project
- **Development/Acquisition:** Designing security architecture, secure code development and implementing security controls against buffer overflow, SQL injection and other possible attacks
- **Implementation Phase:** While performing security test, business goals and conditions must be kept aligned with security goals. A comprehensive change management program consisting of detailed guideline, procedures, approvals, necessary requirements and project deployment should also be developed.
- **Operation/Maintenance Phase:** The required steps in this phase include: periodic based data backups, software patch management, necessary end user training; access authorization process and daily or weekly based activity logs review.
- **Disposal Phase:** The application code should be archived to a secure site or destroyed. All media must be sanitized to prevent the unintended leakage of sensitive or highly sensitive information [21].

4.2 IT Project Management Framework

IT project management framework is based on the design and development of an IT or information system project. IT project management framework covers SDLC phases. Figure 2 below shows the integrated phases of system development and project management lifecycle:

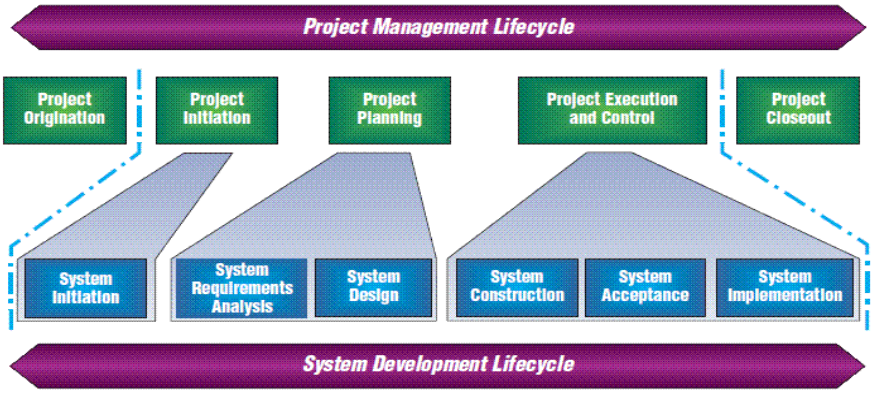

Fig. 2: SDLC and PM integrated lifecycle

Following are the five phases presenting how system development moves through project management. Each phase covers the system development activities [**22**].

- **Project Initiation:** System & user requirements and feasibility study
- **Project Planning:** System design, analysis, technical and functional requirements
- **Project Execution:** System development & coding, unit testing, integration & system implementation and user acceptance & change control/configuration management
- **Project Monitoring and Controlling:** Monitoring and controlling of project covers the performance analysis of the project, to see how well the project is progressing? Is it accomplishing as planned or not? This phase usually doesn't cover any SDLC activity [24].
- **Project Closing:** This is the last phase of a project management where project finalizations get done. It comprises a number of significant tasks including documentation of the overall project and lesson learned for future work. New system replacement with existing system and old system's removal activities get done in this phase [**22**].

5. Proposed Framework

As the aim of this study to present a comprehensive framework of SDLC, PM and IS, though, this section finally presents the proposed framework that demonstrates how security can be integrated at each level of IT project management. This framework consists of ITPM and SDLC phases and shows interrelated security terms for each phase. The framework presented in figure 3 consists of four levels; the first one demonstrates that the CIA triads should be maintained at each level of ITPM security to ensure secure communication and security of the entire project. The second level presents the project management phases that are integrated with the third level of system development. Each level of PM is covering system development phased except execution phase that covers both development and implementation both phases of system development and their security requirements. The last level consists of security requirements need to be accomplished in each phase. The incident handling, business continuity and change control plans developed in second phase should be in place to handle any uncertain situation. Further detail of all integrated phases is defined in table 2 below:

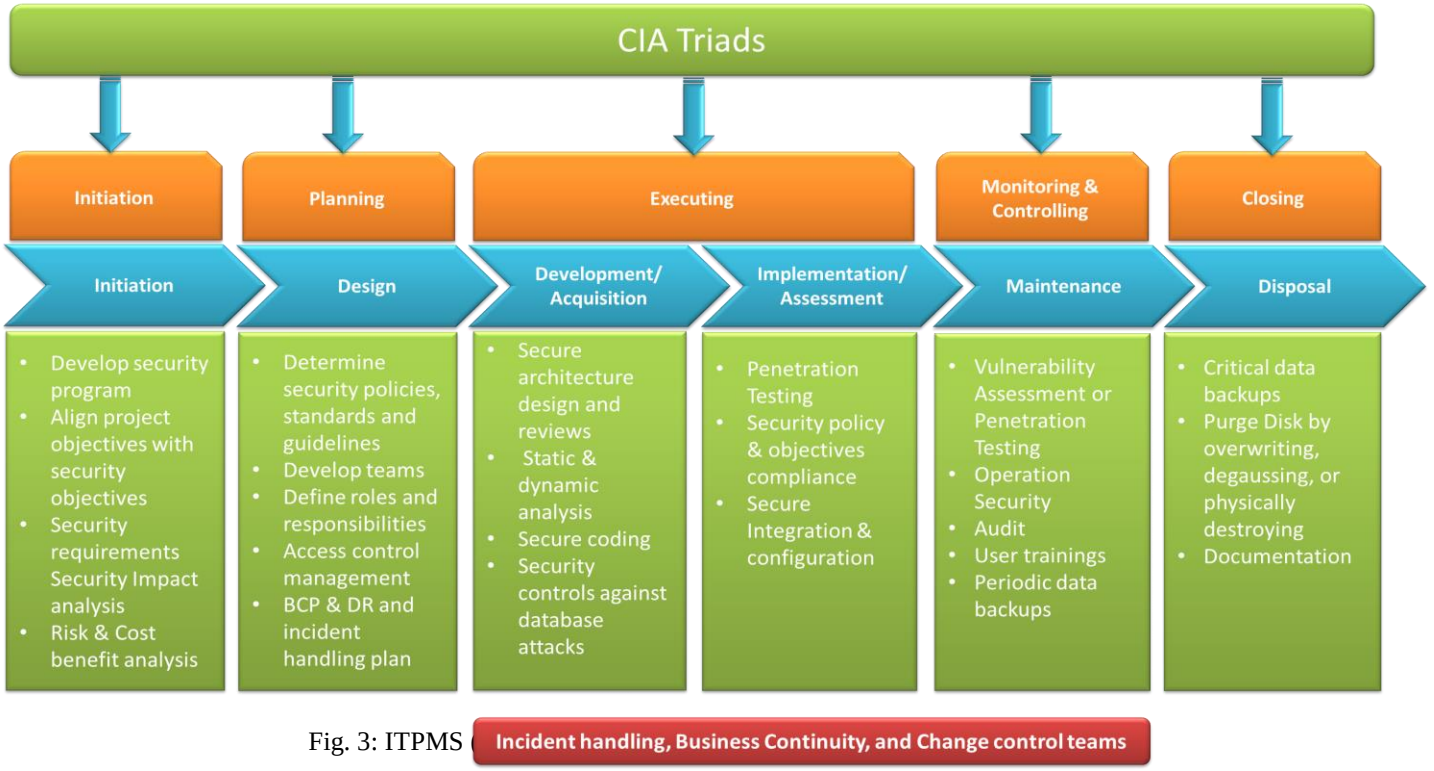

Fig. 3: ITPMS

TABLE 1: Description of proposed framework

System Development	Project Management	Security Controls
Initiation: In this phase system analyst identifies the problems and end solutions, designs SDLC framework and performs feasibility studies.	**Initiation:** It involves the scope of the project, its cost and benefit analysis to agreed stakeholders on secure deliverables.	Security program development and analysis should get done to see security impacts on the project. These include cost/benefit analysis and deliverables. Security objectives should be aligned with project and system objectives.
System Design: System analyst gathers business/user and system (functional & technical) requirements.	**Paining:** Includes planning of deliverables according to financial feasibility, risk analysis, information system management among the team and backup plans.	Design security policy, standards and guidelines so everyone can get direction. Also need to development teams, roles and responsibility assignment. Data classifications and accessibility should also be done, according to their roles. Secure communication by determining communication channels such as secure wireless or VPN (virtual private network) or data encryption. Lastly but most importantly BCP & DR, change control and contingency plans should be developed to handle any uncertain situation or change.
Development/Acquisition: Software developer develops coding, done system configuration, designing user interface and performing unit testing.	**Execution:** It is a functional step that focuses on encryption of passwords and stored data, secure communication, access control, data security and documentation.	Here, IT manager and security expert put all plans into action. They make secure development of the system and perform unit testing to ensure security controls.
Implementation: The all plan, deploys in this phase. A final unit testing is performed to make sure the developed software is error free.		Vulnerability assessment should be performed to see possible errors and flaws against attacks. Other systems and devices should also be tested against

System integration gets done with other systems and devices. All system sign-off if doesn't meet user/business requirements.		attacks before integrating the developed system or software. Change control management should perform in case of required changes.
Operation & Maintenance: Configuration management and required maintenance done in this phase.	**Monitoring & Controlling:** The steps involve includes review and validation of all previously done work and its verification.	User training should be provided if required. Change control management and penetration test should perform after new changes.
Disposal: Old system gets removed or disposed-off to replace new one.	**Closing:** of project, final documentation of the learning and experiences throughout the process.	A backup of critical or important data should be made before removal of the system. Media (hard drive) used for the data should be rewritten by purging or degaussing methods, in order to avoid data recovery.

6. Conclusion & Discussion

The study finally concludes with this point "Whatever you do or build should be protected," said by Dan Emory (a security expert of Netsec). Many organizations today do many projects, but do not follow security standards to accomplish their project successfully. Therefore, any IT project manager that wants to manage projects securely can apply security essentials into project management phases. IS ensures that project is not only secure, but also delivered on time, on budget and according to specifications. As, the best time to address security is before a security risk occurs, thus IT manager should develop a security program with the help of the security professional to reduce security risks as early as possible. It is much far better to implement security than entire project devastated and cause millions dollar loss. It is not a good idea to expect from an IT project manager to develop, implement and maintain a security program. Security is not a single domain, only security experts can fully justify security needs. Hence, if IT manager involves a security expert in every phase of project management, he can rely on him for an uninterrupted, smooth and backed up a project plan. Also, the adoption security practices grounds significant influence on an IT project's success. Besides involving a security expert and three major constraints (cost, quality and time) of management, project managers should also have fundamental knowledge of information security concepts, so they can monitor either security program is being handled accordingly or not. It's also been concluded that the communication has an integral role in the success or failure of project, the first step to secure a project is to create a secure communication plan. For a secure project, not just documents but every single communication among project members should be under strict check of access control and encryption. This could only be achieved by maintaining CIA at every phase of project management. This study explains all aspects of security that defines why security is important for IT project management and how it reduces the project failure chances. There are various studies available that discuss about the integration of system development phases with project management but do not focus on security need. There are no such studies available that shed light on security importance in project management. However, only SANS have one publication "security best practices for IT project managers" that emphasizes on security need in IT project management and only few authors such as Den Emory has published some articles on this. This is the first study that presents this combined framework of project management, system development and information security. Penetration testing and business continuity and disaster recovery management are additional concepts in this study that also differentiate it from SANS best security practices publication.

7. References

s[1] Pruitt Michelle, "Security Best Practices," *http://www.sans.org/reading-room/whitepapers/bestprac*, Oct 2013. [Online]. http://www.sans.org/reading-room/whitepapers/bestprac

[2] SANS, "Security Best practices for IT Project Managers," SANS reading room, 2013.

[3] Dan Emory. (2013) SCMAGAZINE. [Online]. http://www.scmagazine.com/the-need-for-secure-project-management/article/30225/

[4] R. Goatham, "The Story Behind the High Failure Rates in the IT Sector ," 2009.

[5] Lars Mieritz, "Gartner Survey Shows Why Projects Fail," 2012.

[6] IBM. (2012) Faeth Coaching. [Online]. http://faethcoaching.com/it-project-failure-rates-facts-and-reasons/

[7] Robert J. Ellison. (2013) Security and Project management. [Online]. https://buildsecurityin.us-cert.gov/articles/best-practices/project-management/security-and-project-management

[8] B Schneier, "Security ROI," 2008.

[9] Collet Ron Mike Gentile. (2014) Project management as a security touch-point. [Online]. http://www.cisohandbook.com/Default.aspx?tabid=324

[10] S. M., Soomro, T. R., & Brohi Ali, "Mapping Information Technology Infrastructure Library with other Information Technology Standards and Best Practices," *Computer Science*, 2013.

[11] Shon Haris, "CISSP All in one exam guide," 2008.

[12] J Christianson, "Cryptography – Business Value Behind the Myth," 2003.

[13] Paul H. Jacques, & John R. Adams Michael Thomas, "Developing An Effective Project," *Project Management Journal*, pp. Vol. 39, No. 4, 105–113, 2008. [Online]. http://www.pmi.org/learning/developing-effective-project-planning-team-building-5580

[14] C Brodie, "The Importance of Security Awareness Training," *SANS Institute Reading* , 2009.

[15] B. Krenek, "Secure your outsourcing practices to prevent data breaches," 2013.

[16] B. (2012) Krebs, "Exploring the Market for Stolen Passwords," *Krebs on Security*, 2012.

[17] Albert Caballero, "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems," *Terremark Worldwide, Inc.*, 2008.

[18] Jiju (Jay) Nair. (2013) Technology Project Management. [Online]. http://nairjiju.blogspot.com/2013/01/waterfall-is-it-back.html

[19] Kevin Henry, "Penetration Testing, Protecting Networks and Systems ," 2012.

[20] NIST, "National Institute of Standards and Technology Security Considerations in the System Development Lifecycle," 2012.

[21] Kevin Stine & Matthew Scholl Richard Kissel, "Security Considerations in the System Development Life Cycle," U.S. Department of Commerce , 2008.

[22] Roli Pathak, "Top 5 Project Management Phases," March 2014. [Online]. http://project-management.com/top-5-project-management-phases/

[23] N. Nayab, "A Review of Three Project Management Horror Stories and the Lessons We Can Learn From Them," *Bright hub pm*, 2012.

[24] Tom Carlos, "Reasons Why Projects Fail," 2014.

[25] National Security Agency, "Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked environment," , *Information Assurance Solutions Group – STE 6737*.

[26] Jean Scheid. (2012) Bright Hub Project management. [Online]. http://www.brighthubpm.com/monitoring-projects/15893-lessons-we-can-learn-from-three-project-management-horror-stories/

[27] J., Klein, G. and Ellis, T. S Jiang, "A measure od software development risk," *project management*, pp. 30-41, 2002.

[28] Jim Ditmore, "Why Do Big IT Projects Fail So Often?," 2013.

[29] Do you have a Business Continuity Plan (BCP). (2012) Computer Concepts. [Online]. http://www.carolinacomputer.net/do-you-have-a-business-continuity-plan-bcp/

[30] OWASP. (2013) CISO AppSec Guide: Application Security Program. [Online]. https://www.owasp.org/index.php/CISO_AppSec_Guide:_Application_Security_Program