



YONSEI UNIVERSITY
GRADUATE SCHOOL OF INTERNATIONAL STUDIES

IT System Failures: The FBI's Virtual Case File Case Study

2nd Version

Andre Schmitz

Brian Tada

Richard Hess

Global IT Management

Professor Heejin Lee

Yonsei University

Graduate School of International Studies

Seoul, June 17th 2014

Abstract

This paper analyzes the Federal Bureau of Investigation's failed attempt to introduce a criminal case management system called the Virtual Case File (VCF) back in 2005, after investing \$170 million over five years in the project. Thereby, the paper uses a comparative research approach by comparing the reason for failure of the VCF system with its successful follow-up project called the Sentinel. The comparison along four different dimensions including Task, Structure, Actors and Technology has shown that the VCF suffered due to an absence of an enterprise architecture, a poorly designed system, lack of project management skills and a strong dependence on external contractors. Nevertheless, the FBI did learn from its previous mistakes and improved its IT development skill in the Sentinel project, which was successfully implemented in 2012. The results shows that successful IT system implementations need to be based on a clear blueprint, need to be constantly tested and redesigned within the final operational environment, need to be planned and managed carefully and need managers with specific knowledge in IT and project management.

CONTENT

LIST OF FIGURES.....	IV
1. INTRODUCTION.....	1
2. LITERATURE REVIEW AND METHODOLOGY	2
3. THE TRILOGY PROJECT AND THE VIRTUAL CASE FILE SYSTEM	5
3.1. BACKGROUND.....	5
3.2. SYSTEM DEVELOPMENT.....	6
3.3. REASONS FOR FAILURE	8
3.4. INTERIM CONCLUSION.....	11
4. SECOND ATTEMPT: THE SENTINEL PROJECT.....	12
4.1. BACKGROUND.....	12
4.2. REASONS FOR SUCCESS	12
4.3. INTERIM CONCLUSION.....	15
CONCLUSION	16
REFERENCES	18

List of Figures

Figure 1: Historical IT Failure Rates	2
Figure 2: Risk Dynamics during System Development Life Cycle	3
Figure 3: General Research Approach	4
Figure 4: VCF timeline	8
Figure 5: Main reasons for failure	11
Figure 6: Agile Process with integrated Scrum Methodology	15
Figure 7: Comparison of the Reasons for Failure and Success of the two Projects	16

1. Introduction

Information Technology (IT) systems constitute a central component of any modern organization. They are significantly contributing to its success, improve its process efficiency and effectiveness and may even serve as a source of competitive advantage over other competitors. Accordingly, global IT investments in 2013 have been estimated around \$3.6 trillion and are expected to grow by 3.2% to more than \$3.7 trillion in 2014 (Gartner, 2014). Nevertheless, the design, development and implementation of a specific IT system in an organization is accompanied by many uncertainties and not surprisingly, many IT projects fail in being implemented successfully or in the initially desired form.

In this context, this paper analyzes the FBI's failed attempt to introduce a criminal case management system called the Virtual Case File (VCF) back in 2005, after investing \$170 million over five years in the project. The VCF was part of a larger project called Trilogy, which aimed at modernizing all of the organization's IT system infrastructure and applications in order to facilitate more efficient and effective processes (Office of the Inspector General, 2005). This should be achieved in three main steps: (1) Upgrading the FBI's hardware and software (Information Presentation Component IPC); (2) Upgrading the FBI's communications network (Transportation Network Component TNC); (3) Upgrading the FBI's five most important investigative applications (User Applications Component UAC), including its antiquated case management system. The IPC and the TNC would provide the physical infrastructure that is needed to run the UAC.

As the first two components of the Trilogy project were implemented more or less successfully, this paper is only focusing on the key reasons for the failure of the VCF system. In a second part, it contrasts the reasons for failure of the VCF system with the reasons for success of its follow-up project called Sentinel, which was successfully implemented in 2012.

By following this comparative case study approach, this paper illustrates the critical issue areas of IT project implementations and discusses how they can be managed.

2. Literature Review and Methodology

According to the CHAOS reports of the Standish Group, more than 60% of IT projects fail or at least are challenged in being implemented successfully (see Fig. 1). Thereby, the Standish Group defines projects only as successful if they meet the requested functionality within the expected time and expenditures (Standish Group, 2013). Many research efforts so far have supported or complemented these trends and examined the success of IT system implementations based on these three factors: scope, budget and timelines. As the definition of success and failure plays a central role, the results need to be carefully interpreted. Furthermore, it is essential to distinguish between the symptoms and the actual root causes of a project failure. The identified factors for failure need to be critically examined for their significance on the final outcome.

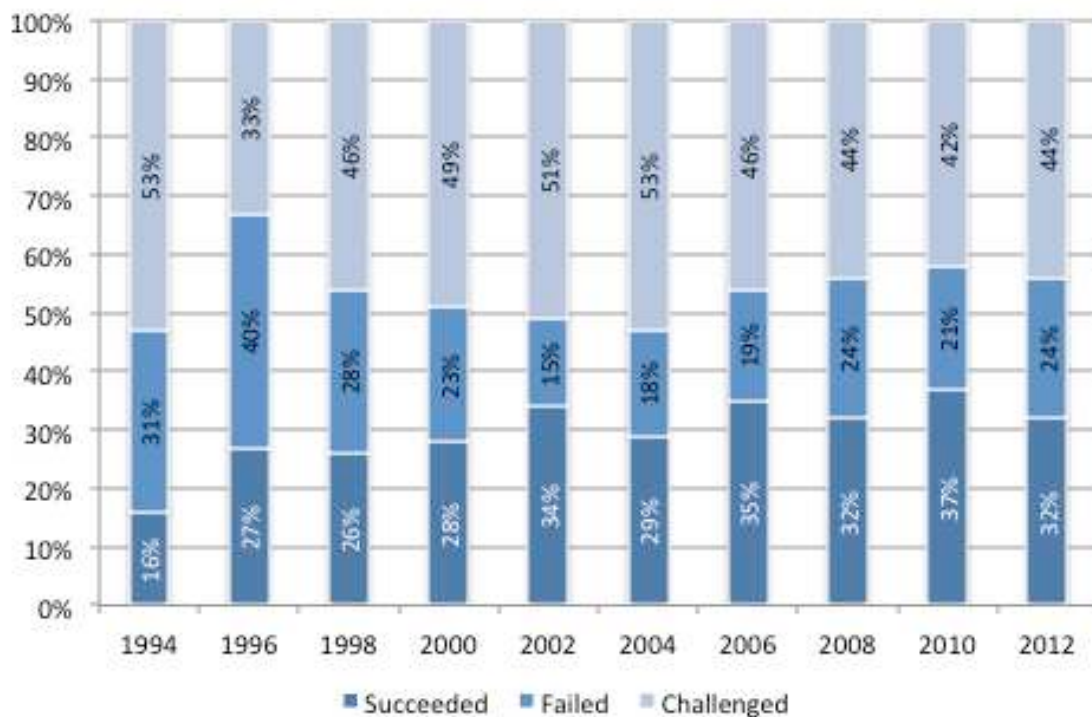


Figure 1: Historical IT Failure Rates

(Source: own Figure, based on data from Stoica & Brouseb, 2013, p. 729)

IT project can fail because of many reasons. In general, there are three approaches to examine these reasons: Technical, behavioral and socio-technical. Each of these approaches emphasizes different factors and thus can lead to different conclusions. In general, they can be categorized into four problem areas: 1) Design, 2) Data, 3) Cost and

4) Operations, whereby the source of failure can be technical, non-technical or a mixture of both (Laudon & Laudon, 2011).

Based on these perspectives, researchers have developed many different models in order to analyze IT implementations. A well-known model, for example, was developed by DeLeone & McLean (1992, 2003). Their model identifies system quality, information quality and IT service quality as the critical factors that lead to the actual use of a system and higher user satisfaction, both causing net benefits for the organization. Other studies examine IT projects within their broader organizational context, by taking into account strategic, political and cultural aspects (Wurster, Lichtenstein, & Hogeboom, 2009). Also, Stoica & Brouseb (2013) suggest a multi-method four-phased research strategy, which offers an unbiased investigation of the causes and interdependencies of IT project failures and how they can be better predicted, prevented, managed and controlled.

For the following paper, the authors will base their general methodological approach on the risk factors derived by Yu, Chen, Klein & Jiang (2013). They identify four socio-technical risk categories (Task, Structure, Actor, and Technology) and apply them along the system development process (Planning, Analysis, Design and Implementation (see Fig. 2). This approach helps to break down the complexities of a case and identify the crucial factors in each stage.

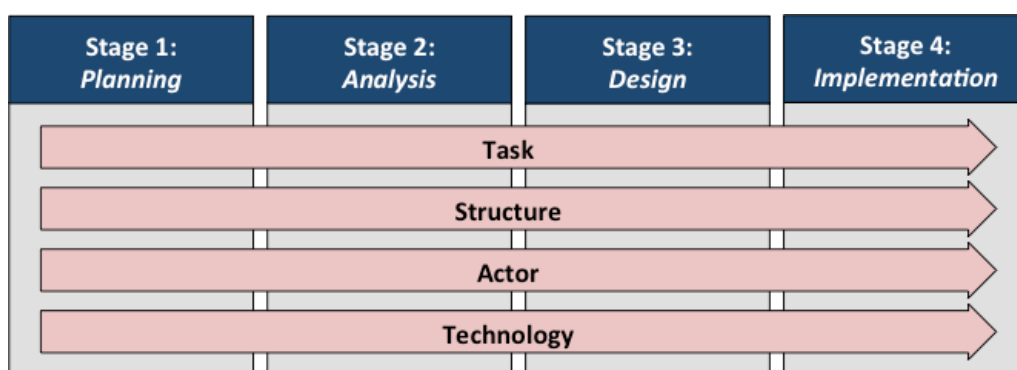


Figure 2: Risk Dynamics during System Development Life Cycle
(Source: own Figure, based on Yu, Chen, Klein, & Jiang, 2013, p. 31).

For the sake of understandability and clear focus of this paper, the authors have adapted the aforementioned model by solely focusing on the four risk categories and analyze each of the two cases along these dimensions (see Fig. 3). Thereby, the two cases are made comparable, which facilitates clearly derived conclusions. Each of the dimension focuses on specific elements of the development process. First, *Task* describes the general goals of the project. It can include project size, number of participants, requirements determination and process results. *Structure* refers to coordination mechanisms and authority relations. This can include poor communication systems, poorly defined responsibilities and unrealistic schedules. *Actor* includes anyone who can affect or is affected by the outcome of a project. It can comprise short of personnel, high turnover rates, poor or inadequate skills/experience or power plays. Lastly, *Technology* covers all the tools, methods, equipment and infrastructure that are used to develop a certain system. This includes the technical user interface, defects, maintainability and extendibility (Yu, Chen, Klein, & Jiang, 2013).

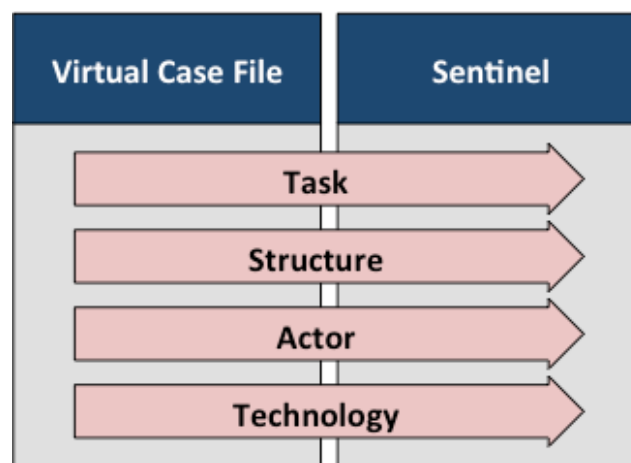


Figure 3: General Research Approach

(Source: own Figure, based on Yu, Chen, Klein, & Jiang, 2013, p. 31).

3. The Trilogy Project and the Virtual Case File System

The goal of the Trilogy Project was to upgrade the IT infrastructure of the FBI and to provide a system, which would allow the entire FBI employees to access the data from any office in its organization. Each computer used to process relevant data and all the software used for these tasks were meant to be linked together using a high-speed network. Through a user application known as the Virtual Case File, every agent would be able to access and analyze the data in this network.

The Virtual Case File was supposed to integrate the primary 40-odd investigative software applications, including the Automated Case Support System (ACS), Intel Plus, the Criminal Law Enforcement Application, the Integrated Intelligence Information Application and the Telephone Application and make these accessible using a point-and-click Web interface.

The following section introduces the background information that lead to the introduction of the VCF systems and analyses its main reasons for failure.

3.1. Background

The project actually began in the 1990's, when FBI Special Agent Larry Depew recognized the need for a database program that would help him and other agents to organize the piles of evidence collected and compiled during their investigations. A huge amount of data from wiretaps, interviews and financial transactions, collected during two and a half years of investigating mafia involvement in skimming off millions of dollars in Federal and New Jersey state gasoline and diesel taxes, were needed to be organized in order to connect only relevant evidence to the case. Following up the paper trail of the Mafia to find the company in the end of the chain, which let the tax free sales of gasoline easily disappear somewhere in Panama, and to prove their involvement in oil cocktailing between local gas dealers and the industry responsible for the processing of the toxic waste throughout the country was just too much of a challenge for the FBI. Too many unconnected, unsorted data showed the need for a better IT infrastructure and organizations. In order to address this challenge, a new system was needed which would become the Virtual Case File (VCF) system project. This system would even enable the

import of information from other investigations to support current investigations. (Office of the Inspector General, 2005)

Even though the FBI was using the ACS, it appeared challenging to connect important dots with that program, especially to the ends that might have not even emerged yet. Among others, the main issues with the ACS were its program language and general database system. It used a program language called natural, an ADABAS database management system and IBM 3270 green screen terminals. This combination of a database system based on a folder and not just an excel-like sorting system with a too complex programming language and an unsuitable IT hardware was inappropriate to get the job done. Hence, the new VCF system would replace the existing ACS, as it was too inefficient and limited in its capabilities in order to solve the current overwhelming tasks. (Office of the Inspector General, 2005)

3.2. System Development

Officially, the VCF project began in 2000, when the FBI began to deal with its outdated IT systems infrastructure. On July 17, 2000, the FBI hired Bob E. Dies to create a plan for this IT transformation. Dies, who was a former executive with IBM, replaced Louis J. Freeh, who unfortunately did not have the necessary IT skills or competencies to complete such a task. Dies was the first of five who tried to solve the FBI's multifaceted task to create an efficiently working VCF system. This led to inconsistencies and caused several problems, as will be explained in the next chapter further down.

Dies presented the prototype of the system in front of the US Senate Committee on the Judiciary in May 2002. During his presentation, he pointed out that they are replacing the antiquated Automated Case Support system in favor of a multimedia, near-paperless Virtual Case File system. Thereby, he emphasized the significant improvements for the FBI's investigation processes and the new capabilities that would reduce the possibility of misfiling or losing future documents. Furthermore, the new system would dramatically decrease the potential of human errors. First, by enabling the automation of many functions so far done manually. And second, by substantially reducing inherent system errors of the ACS system, which caused many problems. At that point, the FBI's computer network was being completely revitalized to provide a better data warehousing and a collaborative environment instead of application stovepipes. This

provided an easier and more robust access to all the necessary systems and improved the capabilities for information sharing. It eventually resulted in the creation of an integrated database and eliminated the need for an ad hoc crisis software application.

Dies further explained that the VCF system would not need dozens of screen entries just to enter one document and upload it into the system. Rather, it was designed to operate on a browser-based point-and-click technology, thus providing a user-friendly and intuitive interface.

For security reasons, access to the VCF would be password-controlled with roll-based authorities. Furthermore, it would audit unauthorized access and possess features for document management control. System-wide activity approval logs which will track documents where they have been throughout the process from creation into the final system, through what approval processes they travel. Furthermore, the system will be able to show us who may have printed a document, who looked at a document, where the document is. When it is needed for discovery, it will be in one place. It can't be misfiled. It can only be printed or burned onto a CD and transmitted to the defense or to the prosecutors. Unfortunately these efforts presented in front of the Congress would not prove successful in its application and integration. (US Government Printing Office, 2003)

Since September 2000, the Congress had approved \$379.8 million over three years for the project. In 2005, Glenn A. Fine, the U.S Department of Justice's inspector general, submitted an 81-page audit of the FBI's VCF project. In his report he described some factors that contributed to the VCF's failure. This conclusion was submitted in the light of the 9/11 terrorist attacks on the World Trade Center. Finally, the project was dismissed in April 2005. Until this point the FBI spent \$170 million on the VCF project. The following Figure 4 shows the key milestones of the VCF's development process.

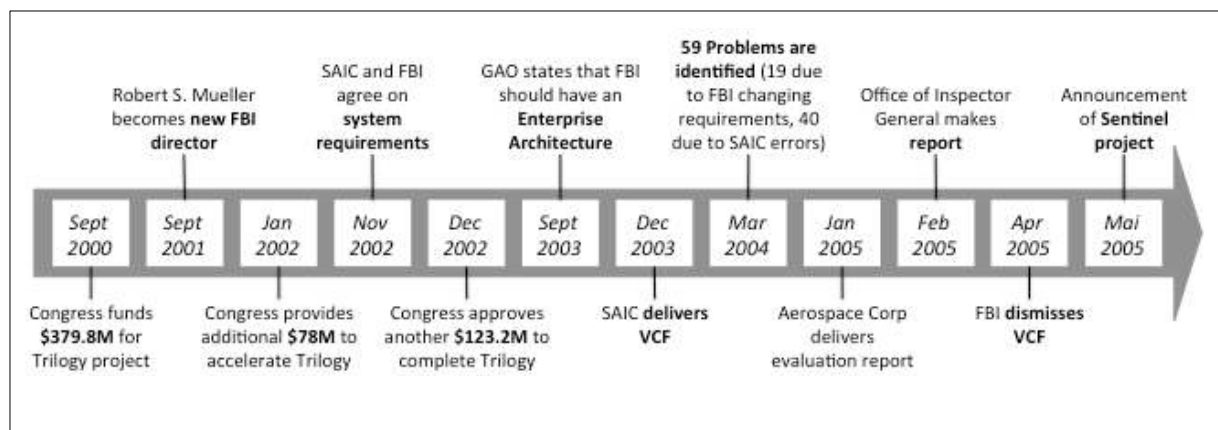


Figure 4: VCF timeline (Source: own Figure, based on Marchewka, 2010, S. 9)

3.3. Reasons for Failure

Even though the need for an IT system upgrade and a more efficient user application for investigations were evident, the implementation of the system failed after five years of development and \$170 million spent. The reasons for failure were broad, but can be summarized into four basic fields of failure: (1) lack of appropriate enterprise architecture; (2) poor system design; (3) poor program and contract management and (4) lack of IT knowledge and human resources. (McGroddy & Li)

Enterprise Architecture Foundation

The purpose of having an Enterprise Architecture (EA) is supporting the information system development and enterprise reengineering. It is a *“a conceptual framework that describes how an enterprise is constructed by defining its primary components and the relationships among these components.”* (Rood, 1994, S. 106). The EA is the backbone for every coordinated IS development and use of shared information systems and data. Without this logical structure and higher-level framework for the information system design, the IS will most likely develop randomly and not in the desired direction.

In the case of the FBI's VCF, the lack of such an EA is visible in various points. First and foremost, the FBI's senior leadership was insufficiently involved in the development of the EA, hence leaving crucial decisions about the key policies, operational priorities and significant tradeoffs between the IT system design and the EA unanswered. Consequently, the FBI didn't clarify its operational needs, which must be the driver of every IT investment. This would include a detailed outline of the FBI's goals, tasks,

strategies and key operational processes. With this approach, the FBI's operational objectives and processes could be linked to the IT strategy and clarify the interconnection between the IT investment and a specific operational objective. Thus, the project would have had a clearer strategic focus. However, the lack of such a clear blueprint from the outset lead to repeated changes in specifications for the system and left the team *"to feel [their] way in the dark"* (Goldstein, 2005), as no guidelines or documentation were available for the FBI's IT development processes.

Systems design

Concerning the system design of the VCF, two major problems can be identified.

First, the initial purpose of the VCF was solely to support traditional criminal investigations. Thereby, the project was well on track. But through its expansion to include intelligence tasks for counterterrorism, the project gained in complexity: At one point, it was estimated, that the software application had over 700,000 lines of code. The different requirements of the two missions (investigation on the one hand and intelligence on the other) lead to design modifications that caused various complications and only evolved slowly, hence preventing a successful implementation of the project.

Second, the FBI chose to use a direct "flash cutover" in order to switch from the old Automated Case Support System to the VCF. This means that there was no limited initial roll out of the application in order to enable an adequate testing of the system in an operational context. Hence, the FBI was implementing an actual prototype throughout the organization, inevitably causing further delays.

Program and Contract Management

Successful IT projects need a well-reasoned application development process that includes internal development plans as well as contracts with supporting organizations. It should take into account possible failures for certain steps and the redesign of the software if necessary. Above all, it is impossible to anticipate all the requirements and specifications beforehand. Hence, the development process should be based on extensive prototyping and usability testing with real users. This fosters strong user feedback and involvement from the very beginning in various dimensions of the development process, like desired functionality, convenience and intuitiveness of the user interface, data entry properties and the necessary network capacity for transferring the resulting data volume in order to guarantee a smooth functioning of the software

under real operational conditions. After all, these steps increase the chance of ultimately meeting the user requirements.

In the case of the VCF, the FBI failed to carry out such an application development process, causing delays and higher costs for the whole project. Both, the contract as well as program management suffered substantial shortcomings. First, the contract schedule lacked specifications, deliverables and commitment to checkpoints. Second, the high turnover rate of key FBI staff further increased the delay and costs of the project. Third, the FBI's senior management failed to carry out important tasks such as identifying key operational processes and defining the IT concept of operations, hence making the organization highly dependent on outside contractors. These lacks of IT investment practices and management weaknesses altogether negatively impacted the development process of the VCF.

Lack of IT Knowledge and External Constrains

The last issue area concerns the actual knowledge and skills of the FBI personal. In order to pursue a successful IT implementation, the staff involved in the development process needs to have profound knowledge and skills in both, IT and project management. But the FBI substantially lacked these human resources and skill base, hence leaving the project development in the hands of FBI personal with no formal training in computer science as managers or engineers. This was especially the case for experienced program and contract managers and a senior IT management team with good communication skills. Furthermore, as mentioned above, the continuous turnover of key staff further slowed down the build up of the required knowledge and skills. Although the organization had access to highly qualified personal by borrowing them from other government agencies or even from the private sector, the overall lack of these human resources and skills hindered the desired development and implementation of the VCF.

Last but not least, the FBI was constrained by external factors that limited its management flexibility. For example, in order to pursue the necessary redesigns mentioned above, the organization needed the explicit approval of the Congress. Thus, the organization was unable to react quickly enough to new requirements and challenges that arise throughout the development process.

3.4. Interim Conclusion

As the four issue areas have shown, the implementation of the VCF was doomed to fail from the very beginning. The failure can be traced back to the lack of basic purpose of the project, as there was no clear outline of the desired final product. Thus, the development process was accompanied by ineffective modifications that didn't focus on the operational needs of the organization and strongly increased the system's complexity. Furthermore, the system was not tested in an operational environment prior to its final implementation, thus leaving critical needs for redesigning and user friendliness uncovered. Finally, the whole process was poorly managed throughout its development, as the involved FBI staff had hardly any knowledge about adequate contract and program management and couldn't react quickly enough due to external budget constraints from the congress. Consequently, the final version of the VCF was implemented with large delays, much higher costs, and minimal user-friendliness. After all, the FBI's agents couldn't profit from the new system, as no improvements in efficiency and effectiveness in the case file management processes were achieved. This said, the VCF could have only been successfully implemented when these critical issues had been settled early enough (see Fig. 5). As the next chapter is going to show, the FBI has learned from some of its mistakes and changed its approach in the subsequent Sentinel Project.

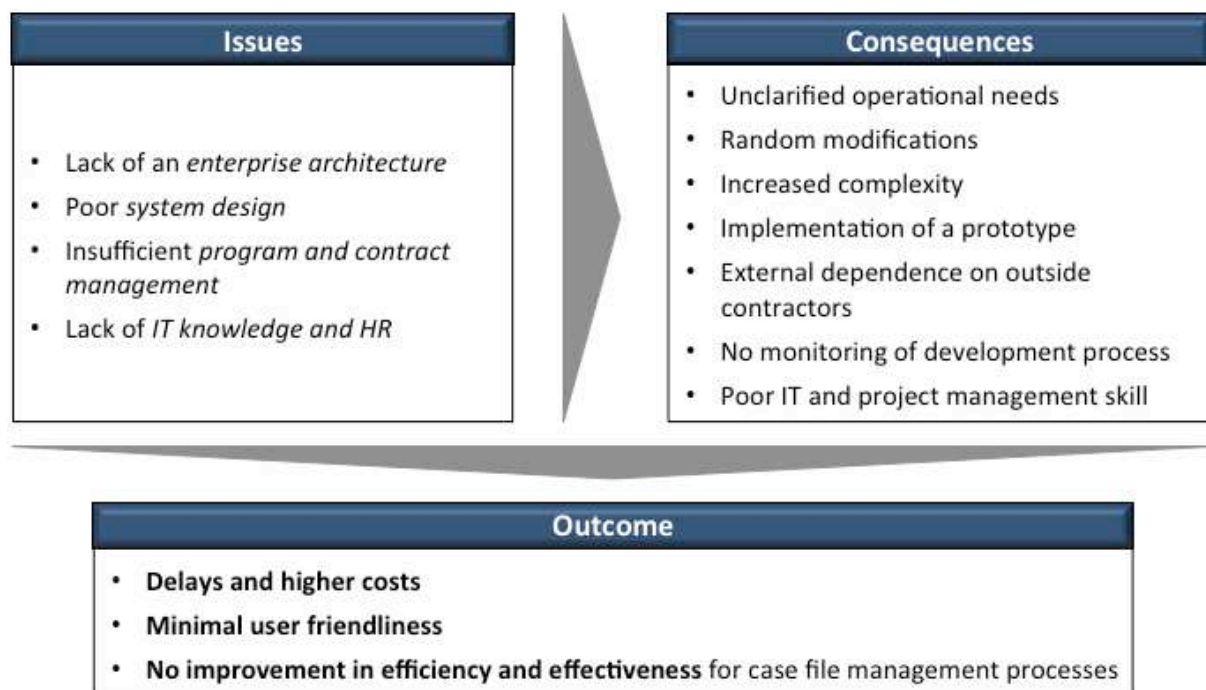


Figure 5: Main reasons for failure (Source: own Figure)

4. Second Attempt: The Sentinel Project

4.1. Background

Sentinel is the FBI's next generation information and case management program that has been in development since March 2006; just one year after the development of the VCF System was abandoned. It is in many ways the successor to the failed VCF Systems. The Sentinel system would once again replace the FBI's aging and outdated ACS System. Sentinel too was set to transform the way the FBI conducted their business by implementing an electronic workflow-based management system of records. Sentinel would also facilitate information sharing with law enforcement and Intelligence Community members. Clearly, Sentinel maintains many of the core initiatives of the original VCF System.

The development of the Sentinel System by Lockheed Martin took nearly 6 years, but Sentinel finally went fully operational in July, 2012. According to data provided by the FBI, the indicators show that FBI employees routinely have been using Sentinel to perform their daily electronic workflow and investigative activities. (The Federal Bureau of Investigation's Department of Justice, 2012, S. 12)

4.2. Reasons for Success

Sentinel's success relative to the VCF System can be attributed to many factors. In essence, the FBI had learned from VCF's previous failures that allowed it to make crucial changes to their approach in the development and implementation of Sentinel. The key reasons for failure- lack of an appropriate enterprise architecture foundation, system design, lack of management skills in contract and program management and lack of IT knowledge were widely addressed in the FBI's second attempt on an electronic workflow-based management system of records.

Enterprise Architecture Foundation & System Design

The main reason often cited for the failure of the VCF System was the lack of focus by the FBI when VCF was in the development stage. The expanding set of requirements by the FBI led to substantial delays and ultimate failure of the system. This was one very important lesson that was learned and used in figuring out the framework and requirements for Sentinel.

From the beginning the FBI defined specific requirements that Sentinel must meet in the Sentinel's System Requirements Specification (SRS) to be considered to be at "full operating capability". The initial version in 2005 contained 1,129 requirements (Interim Report, 2012, p10). As expected, there have been significant advances in technology, IT infrastructure, and the FBI's business processes that led the FBI to reassess and update Sentinel's SRS functionality and requirements.

Instead of continuously adding to the requirements as in the case of the VCF, Sentinel saw an actual decline in the number of requirements to 1,047. 172 were deleted, 119 were modified, and only 90 were added. The FBI stated that it was to clarify and simplify the requirements. This is a significant improvement relative to the FBI's handling of VCF. A crucial aspect to note in requirements is that the FBI narrowed the scope of Sentinel. Some of the deleted requirements were transferred to existing FBI systems. This reduced the complication of development for the Sentinel system. For the FBI, the remaining requirements were the top of their priority list. The deleted requirements could then be later integrated into an already operational Sentinel. (Interim Report, 2012, p11)

Program Management

Sentinel was relatively well managed compared to the previous VCF System. The FBI's Life Cycle Management Directive established in 2006 created policies and guidance for the Sentinel project as well as future IT programs and projects. It contains 23 key processes that manage the development of IT within the FBI. This process consisted of nine phases, seven control gates, and seven project level reviews. To move on to the next phase in development of IT projects the seven gates need to be satisfied. The seven gates are only satisfied by the seven project level reviews. LCMD was designed to ensure that projects meet specific requirements before it obtains management approval to proceed to the next phase increasing control of each IT development.

The FBI also identified 17 key program event milestones and target dates leading to the deployment of Sentinel's final operating capabilities for all end-users. 15 of the 17 were considered completed and 1 in progress as the FBI declared Sentinel "on target" (Interim Report, 2012, p8). This helped to prevent delays in development and implementation of Sentinel. Lastly, Sentinel's early development process was broken down into phases that allowed both the FBI and Lockheed Martin to manage and

examine Sentinel's progress. This broke the 4 phases into segments, each with its own set of checkpoints. (Congressional, 2012, p9)

Overcoming the Lack of IT Knowledge

The main differences are the approach taken in VCF and Sentinel. VFC used the waterfall development model while Sentinel adopted the incremental model. The waterfall development model is centered on the development team. The program is fully constructed and delivered to the end-users as a final product. This allows for very little end-user input/criticism. Learning from their failed VCF system, the FBI implemented the incremental model. This allowed for better communication between end-users and the IT development team.

In this incremental model the FBI took majority of control in the final stage of the development and implementation. Unlike the VCF, which left the development and implementation of VCF largely to the hired developers, Sentinel adopted the Agile approach.

The Agile approach to software development focuses on frequent delivery of capabilities through close collaboration of users, stakeholders, developers, and testers. End user experience and value creation are key factors in implementing the Agile approach. The FBI addressed functionalities in two-week development increments called "Sprints". Each sprint provided vital, quick, and responsive information that could be incorporated into the next set of sprints. This key change insured that the development of Sentinel fit the needs of the FBI agents. (Interim Report, 2012, p13)

In 2010 they introduced the Scrum methodology in conjunction with their Agile approach. This approach involves working in small teams to deliver regular updates to the system. Scrum allows for further fine-tuning within each two-week sprint. Scrum coupled with Agile ensured that the latest technologies and best practices are integrated into Sentinel's development process to address remaining requirements. The two integrated processes are highlighted in Figure 6.

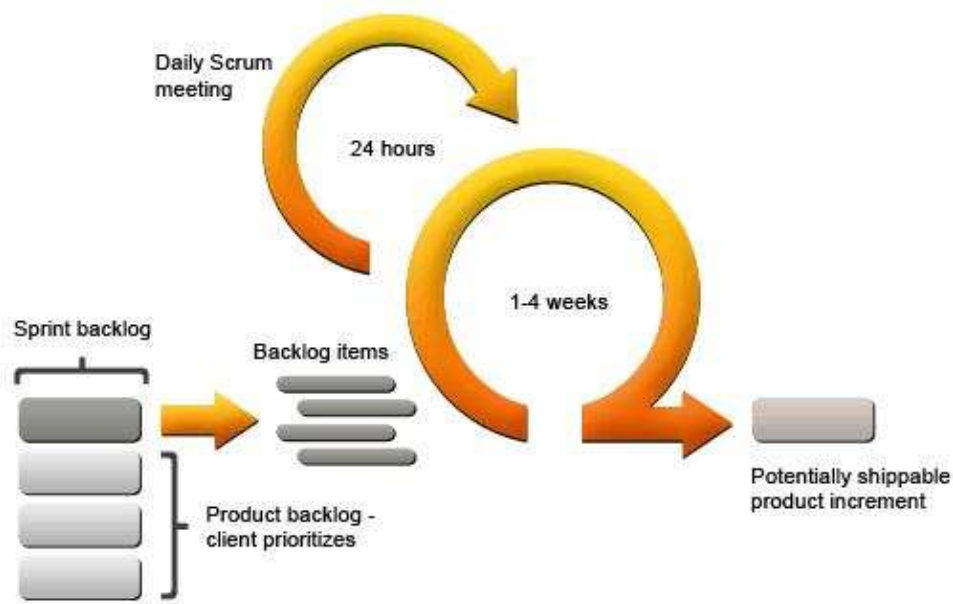


Figure 6: Agile Process with integrated Scrum Methodology

Source: (EnvisionIT, 2013)

4.3. Interim Conclusion

Sentinel has attained relative success due to the lessons learned from the FBI's failure of the VCF System. Narrowing system requirements to clarify and simplify Sentinel help keep down the cost and complication. This provided a better framework for developers. Establishing the Life Cycle Management Directive helped the FBI to better manage and direct the flow of its IT development. Breaking down Sentinel into development stages also allowed better micromanagement, making sure Sentinel stayed within its goals and timeframe. Lastly, adopting the Agile approach allowed Sentinel to develop with the feedback of its end-users. These factors have largely contributed to not just lower its overall cost but also the successful implementation of the Sentinel project as design and developed to best fit the needs of the FBI. (EnvisionIT, 2013)

Conclusion

This case study has shown that IT projects are often times accompanied by various complications and downturns. By comparing the failed implementation of the VCF with its subsequent successfully implemented Sentinel project in four different issue areas (Task, Structure, Actor, Technology), the paper could identify several key factors that need to be considered when implementing an IT system implementation (see Fig. 7).

Factor		VCF	Sentinel
Task	Enterprise Architecture	<ul style="list-style-type: none"> No pre-defined EA and guidelines No clarification of the FBI's operational needs 	<ul style="list-style-type: none"> System Requirements Specifications (SRS)
Structure	Program and Contract Management	<ul style="list-style-type: none"> External dependence on outside contractors No monitoring of development process 	<ul style="list-style-type: none"> Life Cycle Management Directive Definition of key milestones Incremental development methodology FBI took direct supervision
Actor	IT Knowledge and HR	<ul style="list-style-type: none"> Poor IT and project management skills No sharing of best practices and experiences 	<ul style="list-style-type: none"> Agile and scrum approach Close collaboration of users, stakeholders, developers and testers Integration of latest technologies and best practices into Sentinel's development process
Technology	System Design	<ul style="list-style-type: none"> Expansion of purpose Random modifications, increasing complexity "Flash-cutover" 	<ul style="list-style-type: none"> Clear defined system requirements Clarification and simplification of requirements during development process

Figure 7: Comparison of the Reasons for Failure and Success of the two Projects
(Source: own Figure)

This comparison allows deriving critical lessons learned for future IT implementations.

First, *IT projects need to be based on a clear blueprint*. This serves as the backbone of the project and helps to narrow down the requirements. Without such enterprise architecture, IT projects are likely to lose their initial focus and become too complex due to ineffective modifications.

Second, *IT projects need to be constantly tested and redesigned within the final operational environment*. This helps to identify problem areas that need to be solved and keep a user-friendly interface.

Third, *IT projects need to be planned and managed carefully*. Developing the system step by step can help to identify and solve possible errors quickly and effectively, which

And finally, *IT project managers need specific knowledge*. This includes both, sufficient IT knowledge as well as project management skills to be able to understand and support the whole development process.

These findings can be generalized widely to any IT project in any industry or business. However, the comparison with other failed IT projects will certainly reveal other key issues areas. Therefore, these findings only show an excerpt from a wider set of reasons for why and how IT projects fails. Nevertheless, they certainly help to improve the ability and likelihood for successful IT project implementations.

References

- DeLone, W., & McLean, E. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research* , 3, pp. 60-95.
- DeLone, W., & McLean, E. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management information Systems* , 19 (4), pp. 9-30.
- EnvisionIT. (2013). *Agile Project Managment Process*. Retrieved April 25, 2014, from <https://www.envisionit.com/products/aboutus/Pages/Agile-Process.aspx>
- Gartner. (2014, April 2). *Gartner Says Worldwide IT Spending on Pace to Grow 3.2 Percent in 2014*. Retrieved June 14, 2014, from Gartner: <http://www.gartner.com/newsroom/id/2698017>
- Goldstein, H. (2005, September 1). *Who Killed the Virtual Case File? How the FBI blew more than \$100 million on case-management software it will never use*. Retrieved April 23, 2014, from <http://spectrum.ieee.org/computing/software/who-killed-the-virtual-case-file>
- Laudon, K. C., & Laudon, J. P. (2011). *Management Information Systems: Managing the Digital Firm* (12 ed.). Pearson.
- Marchewka, J. T. (2010). *The FBI Virtual Case File: A Case Study*. Retrieved April 15, 2014, from http://www.iima.org/index.php?option=com_phocadownload&view=category&download=270:the-fbi-virtual-case-file-a-case-study&id=48:2010-volume-10-issue-2&Itemid=68
- McGroddy, J. C., & Li, H. S. *A Review of the FBI's Trilogy Information Technology Modernization Program*. Committee on the FBI's Trilogy Information Technology Modernization Program . Washington D.C.: National Research Council.
- Office of Inspector General. (2012). *Interim Report on the Federal Bureau of Investigation's Implementation of the Sentinel Project. Report 12-38*. Retrieved April 15, 2014, from <http://www.justice.gov/oig/reports/2012/a1238.pdf>

-
- Office of the Inspector General. (2005). *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*. Retrieved April 8, 2014, from <http://www.justice.gov/oig/reports/FBI/a0507/>
- Rood, M. A. (1994). *Enterprise Architecture: Definition, Content, and Utility*. Retrieved April 23, 2014, from IEEE:
<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=330494>
- Standish Group. (2013). *CHAOS Manifesto 2013: Think Big, Act Small*. Retrieved June 14, 2014, from
<http://www.versionone.com/assets/img/files/CHAOSManifesto2013.pdf>
- Stoica, R., & Brouseb, P. (2013). IT project failure: A proposed four-phased adaptive multi-method approach. *Procedia Computer Science*, 16, pp. 728 – 736.
- The Federal Bureau of Investigation's Department of Justice. (2012). *Congressional Report on the Federal Bureau of Investigation's Next Generation Information and Case Management Program*. Retrieved April 15, 2014, from
<https://www.hsdl.org/?view&did=739465>
- The Federal Bureau of Investigation's Management of the Trilogy Information Technology Project. (2005, February). *Findings and Reccomentations*. Retrieved Arpil 26, 2014, from
<http://www.justice.gov/oig/reports/FBI/a0507/findings.htm>
- US Government Printing Office. (2003). *Reforming the FBI in the 21st century: Hearing before the Comitee on the Judiciary United States Senate*. Retrieved Mai 31, 2014, from <http://www.gpo.gov/fdsys/pkg/CHRG-107shrg88571/html/CHRG-107shrg88571.htm>
- Wurster, C. J., Lichtenstein, B. B., & Hogeboom, T. (2009, MaJ/June). Strategic, Political, and Cultural Aspects of IT Implementation: Improving the Efficacy of an IT System in a Large Hospital. *Journal of Healthcare Management*, 54 (3).
- Yu, C.-I., Chen, H.-G., Klein, G., & Jiang, J. J. (2013). Risk Dynamics Trhoughout the System Development Life Cycle. *Journal of Computer Information Systems*, pp. 28-37.
-