AGLPM4 – Unit 4 - ACTIVITY 2: OBSERVE
Case Study 3
Federal Bureau of Investigation - FBI

This document is an excerpt from the book:
“Agile Project Management for Government “
Authored by Brian Werham
Published by Maitland & Strong
Reproduced with permission under license

PMCAMPUS.com / Mokanova Inc
.

Case Study at the FBI

> *One of my arguments is that we've got to have stronger engineering in government. It turns out that in the FBI, the number of really good software engineers is limited, like it is in most federal agencies.*[1]
>
> Jack Israel,
> former FBI Chief Technology Officer

Many organizations need to integrate their activities and create a database of consistent and instantly available information. It seems logical to spend a great deal of time creating a Big Design Up-Front (BDUF), and then check it thoroughly before starting to develop a solution. However, as this case study shows, that waterfall approach created a culture of procrastination and delay at the FBI that the adoption of the agile approach eventually overcame. It shows how you can use an agile approach to save failing projects – no matter how large.

This chapter analyzes a situation where the use of a prime contractor did not absolve a government from managing its risks – it merely exacerbated them. In cases such as this, it is not only more expensive, but also more risky to rely on hands-off management of the development team. In this case, a bloated $482m project failed to deliver until the FBI took direct control of development and adopted an agile approach. Moreover, with that smaller, smarter team, they started to deliver.

Here I further the argument that audit recommendations, overlarge procurements, and ‘best practice’ can be major institutional inhibitors to adoption of the agile approach. Governments must address these factors if they are to become agile. This case provides an example where the US Office of Management and Budget (OMB) and GAO initially reinforced the waterfall culture at the FBI bringing about a massive procurement that failed.

At the end of this case study, I provide some thought-provoking questions that encourage you to re-visit the text. I encourage you to get interactive with other readers and *tweet* your thoughts on these questions using the text #APMFG in your message.

Background

In 2000, the FBI was using old technology – the Automated Case Support (ACS) system – and had to rely upon ad-hoc processes to share documents, photos, and other electronic media. The FBI’s handling of the Oklahoma City Bombing case between 1995 and 2001 highlighted the deficiencies of the technology.

On May 8, 2001, just one week before the scheduled date of the execution of the bomber, the FBI revealed to the defense attorneys that it had not disclosed over 700 investigative documents to the defendants. The FBI processed a tremendous volume of material and sent it to the Oklahoma Bombing investigation task force, but in many cases, the FBI did not send material or lost it.

The legal process was thrown into turmoil, and a stay of execution of the death sentence of one month was granted. The FBI came under severe criticism and allegations were made that FBI personnel may have intentionally failed to disclose the information. However, an independent investigation showed that the combination of the "antiquated computer system" and "human error" were to blame. The ACS did not support the critical operational processes and was difficult to use.[2]

The Trilogy VCF Project Is Set Up

The FBI set up a project to build a Virtual Case File (VCF) system to replace the old Automated Case Support (ACS) system as its primary investigative application. The goal of the VCF was to reduce agents' reliance on paperwork and to improve efficiency by allowing agents to scan documents, photos, and other electronic media into a secure, centrally available, electronic case file.

The development of the VCF was part of the overall Trilogy program, approved by Congress in November 2000. Trilogy aimed not only to implement the VCF but also to upgrade the FBI's IT hardware and infrastructure. The requirements for the VCF were to be agreed up-front by experts. The FBI was to commission its build in a massive contract, and, when it was ready, it would be implemented in a full-scale big-bang rollout.

It was a classic waterfall project, with an original planned implementation date for May 2004. However, political pressure was applied after the September 2001 attacks, and the FBI made promises of faster deployment. First, the FBI promised completion for June 2003, then December 2002, and finally (after receiving $78m of supplemental funding on top of the original $379m) for July 2002 at a cost of $458m.

The Trilogy VCF Plans Start to Unravel

The classic symptoms of waterfall project failure started to reveal themselves. Project plans were found to be unrealistic, and the oversight of project spend was inadequate. Although total spend was being tracked, it was not possible to tell whether the project was over or under budget. However, it became obvious that the project would not meet its accelerated deadlines. A commitment to using unproven *thin client* technology was made, and the design for it to allow web-like access to a central case management system was deeply flawed. Up-front contracts with suppliers bound the project to this technology. The first step was to be the web-enablement of ACS. In parallel, and before the technology could be proven, both the hardware upgrade and the new functions made great use of thin client technology. Unfortunately, the project team had not fully explored the security and performance requirements with the users. As these became evident, a total re-write of the programs was required.

Even with the additional $78m of funds, the project missed its July 2002 milestone. Audit reports took a traditional view of what was wrong: more discipline was required. If only processes for tracking and oversight of costs could be made tighter and more detailed. If only more planning and scheduling could be carried out. If only the business requirements had been identified in more detail at the beginning…

The thinking of the auditors was that more detail and planning would have averted the problems. It did not occur to them that over-detailed planning without sufficient real-world feedback was a cause of failure.

The FBI appointed a new Trilogy project executive, hoping that he would recover the Trilogy project using more "structured oversight". Therefore, the July 2002 deadline then slipped from October 2002, to March 2003 and then to June 2004.[3]

The Trilogy VCF Project Is Abandoned

The Trilogy project failed to deliver the VCF, and $170m was written off when the project was canceled in 2005 after having only completed the more straightforward tasks of hardware and network upgrade.[4]

Auditors applied a waterfall perspective in analyzing why the project failed. Their comments pursued the line of thought that if more detail had been planned upfront, with a stricter set of waterfall processes, then failure would not have occurred. Examples of their conclusions included many possible reasons for the failure:

> "(The project had) poorly defined design requirements, a lack of mature management processes, high management turnover, poor oversight, and significant turnover of project management. 15 different key IT managers over the course of its life, including 10 individuals serving as project managers for various aspects of Trilogy … and five different Chief Information Officers … and a lack of a mature Enterprise Architecture … a lack of specific completion milestones, review points, and no penalties (for suppliers) if milestones were not met." [5]

However, the one factor that the auditors did not consider was whether even more upfront planning and design could fix a broken waterfall model.

The Second Attempt – the Sentinel Project

In 2005, the FBI was still relying on its increasingly outdated ACS case management system and complicated manual procedures. Therefore, plans were drawn up for a new project, to be called Sentinel. The aim, as with the canceled Trilogy VCF project, was to create a web-enabled case management system and to develop it using a waterfall approach based on a Big Design Up-Front. Just as with the previous Trilogy VCF project, Sentinel would take years to develop. Therefore, in the meantime, the users would be given web-based screens to hide the old, difficult to understand mainframe screens. Behind the scenes, data would still be processed by the old ACS system. Despite the new web-based user interface, and a better search facility, no new data capture or sharing functions would be added until the whole VCF was ready.

The project paid very little attention up to this point to planning the necessary changes in business processes to take advantage of the new system. Phase One had been simply the replacement of the displays on the ageing ACS with more user-friendly screens. No significant new functions were to be introduced – it was mainly a like-for-like replacement of features.

Jack Israel, the Chief Technology Officer at the time explained that:

> Some called it *lipstick on a pig* because (the screens just) … allowed agents to interact with … ACS's functionality through a Web browser. It was expensive lipstick, about $60m worth.[6]

Sentinel was to be implemented in four overlapping phases: each 12-18 months long, with the last phase to be completed by 2009:[7]

- ♦ Phase One to reach completion in April 2007 to provide a web-based portal to the ACS (as previously attempted in the abandoned Trilogy VCF project) and some rudimentary case management and indexing facilities
- ♦ Phase Two to implement document management with an electronic records repository with some workflow tool support to ensure correct review and approval
- ♦ Phase Three to provide an improved search facility across all the data
- ♦ Phase Four to complete the task tracking and reporting functions, and to transfer data from the ACS and turn it off.

In addition to developing its Sentinel case management system, the FBI also led the inter-agency Federal Investigative Case Management System (FICMS) initiative to ensure the sharing of case management data across agencies. The need for these interfaces, just as with the VA, would cause problems. Upfront work had not thrashed out the potential problems.[8]

The auditors were hopeful that the new Sentinel project would address previous attempts to implement an up-to-date case management system. They felt that the institution of the waterfall life cycle described in a "Life Cycle Management Directive" would reduce risks. More detailed design and planning would occur up-front, with a comprehensive *enterprise architecture* acting as a detailed blueprint for the future IT environment. The contract was based on a standard National Institutes of Health contract commonly used in US government procurement. The process required the government to assess the suppliers' proposals against theoretical statements of work and project schedules. This type of contract had "proved problematic under Trilogy" when the FBI had rewarded the supplier for meeting goals in project management, cost management, meeting the schedule, and technical performance, not for flexibility, or for the achievement of business benefits.[9]

On March 16, 2006, the FBI awarded a contract to Lockheed Martin Services to develop the Sentinel system by December 2009. The total project budget was $425m, made up of a cost of $305m for Lockheed Martin and $120m for the FBI to run a massive *program office* to carry out detailed and prescriptive oversight of the work.[10]

Project control was set up in a traditional waterfall fashion. The specification was fixed at the beginning and spend was allowed to vary. The initial estimates could not be validated, so a contingency of 15% overrun in costs was allowed for. The project manager was optimistic and considered this more than adequate, since "based on his experience, an 11% reserve would be adequate".[11]

There was considerable confidence that risks could be averted. So much so, that four of the top five project risks had no contingency plan. It was assumed that little could go wrong, even though the project schedule was based on an early, hypothetical schedule of "dictated milestones" created by the FBI during the procurement – not by Lockheed Martin who actually had to carry out the development work.[12]

The first phase of Sentinel, delivered two months late in June 2007, did provide what seemed like adequate "lipstick on the pig". However, it lacked 57 promised features, such as the ability to open and close cases. The project had not carried out the planned data cleansing activities. The data on ACS was still in a mess, and the team had not yet migrated it over into a test database. This was a key task that would have flushed out the technical difficulties in advance of Phase Two. Despite this, the FBI paid Lockheed Martin as if the phase was 100% complete.[13]

After a few months or so of using the Phase One system, some users were beginning to abandon its use. There were many features which had not yet been catered for (such as opening and closing cases), and many users had switched back to using the old system. Usage had declined by 25% in the six months since implementation.

An audit report issued at this time, however, was optimistic, stating that:

> "The FBI has made considerable progress in establishing controls and processes required to adequately manage a major IT development project such as Sentinel and to bring it to a successful conclusion – if the processes are followed and controls are implemented as intended." [14]

The New CIO Breaks Sentinel into Phases

In December 2008, Chad Fulgham was appointed as the new CIO. He came from Lehman Brothers, and brought a business mentality with him that favored quick results rather than drawn-out planning.[15] Fulgham decided to carry out a strategic replanning. Phase One had taken over a year before the first output – expectations now changed, and he now planned for outputs every 3–6 months.[16] The FBI had initiated a Business Process Reengineering (BPR) effort in 2005, but the Sentinel project had not yet taken this work into account. Fulgham now incorporated these changes to ensure that Sentinel would meet the organization's changing needs.[17]

As work started on Phase Two, Fulgham was publically optimistic about progress, claiming that the four increments of Phase Two constituted an agile approach:

> "This more flexible and agile approach was thoughtfully planned, and further reduces the risk by shifting more of the requirements forward into the program's development.
>
> "Phase two is now more than halfway complete, and is on schedule and within cost. It will also deliver administrative case management services well ahead of the original schedule.
>
> "Among the original goals of the Sentinel program were agility, and the ability to make adjustments during the multi-phase, four-year period – both to account for expected advances in technology and to implement lessons learned along the way. By any measure, the *replant* has made Sentinel stronger and more responsive to the needs of users – those FBI employees who rely on cutting-edge technology to help keep America safe." [18]

The Project Does Not Deliver Iteratively

The replanning effort prior to starting Phase Two had created a gap in the action. Phase One had been completed in June 2007 and Lockheed Martin was only given permission to proceed four months later. The end-date for the whole project now had to slip by six months to June 2010, and projected costs had increased by $30m.

Phase Two of Sentinel did not go according to plan. As functions were delivered, the users found that they did not meet their requirements, and the technical approach needed to be reworked again. The end-date of Phase Two slipped, the cost increased by $18m, and the security and authentication functions were not delivered. Because the new system required a better network infrastructure, some users had reported that it could take up to 30 minutes just to login to the system, so an additional $39m was spent to improve and streamline the network.

The end-date of the Sentinel project now slipped by another three months to September 2010.[19]

A rigid and hierarchical project reporting structure called a Project Management Office (PMO) had been set up. It was large, unwieldy, and exhibited a huge *optimism bias* in its status reporting. Its bloated $120m budget was spent on inexperienced project managers with general government administration backgrounds. They had received basic training, but had little or no background in technology development. Throughout the project, the reports produced by this PMO, despite being detailed and full of statistics, never reported even one sub-project as being in trouble, even as the project was obviously out of control.[20] As late as December 2009 the FBI was still "expecting to provide capabilities to users sooner than originally planned".[21]

Users rejected Segment 3 of Phase Two during testing, even though it was theoretically compliant with the FBI's specifications. They required a complete redesign of the screens. Despite these problems, the FBI Project Management Office (PMO) remained optimistic, with project status reports showing "a horizontal thermometer, which expressed the project's overall status in red, yellow, or green. From meeting to meeting, the temperature never changed—it was always yellow, trending toward green." [22]

However, the more difficult tasks were left to the end. Important tasks, such as developing the migration processes, were left until the end of the phase. Migration was known to be a key problem. Names, addresses, and phone numbers in the old ACS system did not match the format specified in Sentinel's database. In the end, the data migration processes and interfaces took two years to create, and when delivered in 2010 they were still not adequate.[23]

Sentinel Phase Two Is Stopped

Then on March 3, 2010, the FBI decided to reject the deliverables from the fourth and final segment of Phase Two because of continuing usability, performance, and quality problems. The FBI issued an order to Lockheed Martin to stop development on future phases until the problems were resolved. The FBI could now not be sure that the system would meet user requirements, and could not agree with Lockheed Martin how the project was to proceed. The viability of the September 2010 end-date was called into question.[24]

Not only were some of the essential functions still missing, there were also significant performance issues. These were not just due to poor network infrastructure, but also to poor quality in the coding of the software. In some cases, users could create and use fake identities when signing documents electronically.[25]

In July 2010, more functions were delivered to FBI agents to use, but the system still only had the capability to process four of the 18 forms, and these only partially.

Because of Sentinel's delays and cost increases, in July 2010 the FBI issued a complete stop-work order.[26]

An independent report estimated that completing Sentinel under the current development approach would cost at least an additional $351m on top of the $405m already spent, and take another six years. In addition, the risks of working to an outdated specification now loomed. Some of the redesigned BPR processes were now six years old. Technology had moved on, and there had been significant changes to the FBI's work processes that made them outmoded.

The Sentinel system that had been implemented so far was little used by FBI staff. Where it was, it merely resulted in duplication of effort, because data still had to be double-keyed into the ACS. Confidence in the system was so low that its use was officially optional. Between July and August 2010, only 132 new cases were generated in the Sentinel system. This was less than 1% of the 14,831 cases entered into the ACS in the same period.[27]

By now, FBI agents should have had a case management system with workflows for managing their work – instead they were continuing with the same time-consuming, paper-based case management processes that had threatened the Oklahoma Bombing judicial process. The promise of electronic information sharing both within the FBI and to and from other federal agencies to "connect the dots" between cases and suspects had not been realized.[28]

Sentinel Recovers Using Agile Approach

In September 2010, the FBI announced that it would take direct management of the development of Sentinel and use an agile project approach:

> "The FBI made a difficult but sensible decision to develop an alternative plan for completing Sentinel. We examined several options in detail, and selected an approach based on what is known as "agile development" method. This approach will reduce our reliance on traditional contractors and allow for cost-savings by dealing directly with product experts." [29]

The migration of the 8.3m live, cold, and closed cases from ACS to the Sentinel database was in doubt. If it did not work, then ACS would have to remain alive for many years, and FBI agents would have to work with two separate case management systems at the same time. An automated facility to "join the dots" between new and cold cases would not exist.[30]

The existing requirements were analyzed, prioritized, and sequenced to focus on the most valuable requirements with the greatest benefits to agents and analysts.[31]

Within a month, the FBI took direct control of development, removed all Lockheed Martin personnel from development work on the project, and started to supervise the sub-contractors directly. Fulgham reduced the team from over 125 heads to just 55.[32]

The project adopted the Scrum method, with a *Scrum Master* coordinating the development team. This is a role different from that of a project manager in a waterfall project. The Scrum Master leads and enables the team, rather than 'managing' it. They empower a self-organizing team, rather than imposing structure on it.

The original, monolithic requirements document was modularized into 670 separate user stories. The team prioritized each user story in a *product backlog*, each one describing just one end-to-end process that the system needed to do.

Work now started to develop these user stories incrementally. Each cycle of work (or *sprint*) was two weeks long. At the end of every sprint, all testing had to be complete. The software had to be demonstrated to project stakeholders, and ready for deployment to users if required. 21 sprints were planned to develop all the user stories. Although there was concern that a continual churn of changes could ensue, the brevity of the 10-day sprints kept the danger of uncontrolled changes to what the FBI called "just 9 days of risk". Previously, arguments over change control and *scope creep* took up much more time and effort than that.[33]

At the start of each sprint, the development team identified which stories they were to develop during that sprint, and these formed a work plan called the *sprint backlog*. At the end of each sprint, regardless of whether all work was complete, the development team had to test and demonstrate the system. The team could only claim those stories that passed tests as completed. Where a test failed, that user story was placed onto the product backlog for rescheduling into the next or some other future sprint.[34]

The amount of work required to develop each user story was initially estimated as a number of *story points*. These story points were a relative measure of difficulty and size. As work progressed, the team could see how fast they were working, and could start to *calibrate* their efficiency. After a few sprints, it became possible to forecast the rough timescales and start to plan the dates for incremental implementation. This was to be in two increments, with about half the user stories implemented in September 2011 and the rest in November.

However, concerns were raised about the first implementation being near to the tenth anniversary of 9/11 – potentially a time of heightened security. Therefore, the team carried out additional testing which showed that although Sentinel now had adequate functionality and usability, there were still concerns about its performance and availability. The implementation was then planned to be phased in alongside the standard five-year refresh of computer hardware.[35]

In the full year to 2011, only 52% of the much reduced agile development budget of $32.6m had been spent to build 88% of the system.[36] Jack Israel later commented on this success:

> "Agile is not just a method or a process, it's a way of being. You don't *do* agile. You *are* agile. The FBI has arranged to loan their Scrum Master to other teams to get them trained. Increased transparency has kept stakeholders in sync. Further, stakeholders would modify their expectations, based on the increased visibility of the process." [37]

By June 2012, the revised technical targets had been met, and two releases had been achieved. There was a substantial increase in information sharing of case management information and a resolution of IT problems. $46m had been spent on making progress over the last 12 months, and most importantly, agents were now using the system on real cases. 13,268 agents created 623 documents and made 92,546 searches in the first quarter of 2012, against targets of 11,000, 550 and 77,000 respectively. The key operational target of 13,200 leads per quarter in the full year 2012 was missed by a whisker (1% short of target).[38]

In the first release, seven functional areas had now gone live, including allowing different user roles, storing attachments for sharing, and automatic routing, workflow and notifications of urgent actions needed on cases. The second release was a fully functional pilot of more functions at selected FBI field offices.[39] User feedback was positive, and full Operational Capability was achieved in May 2012. We will not know the actual business benefits from the new operational processes until the new Sentinel system beds in after the final user of ACS logs off in 2013.[40]

Conclusions

The cost of the initial failed Trilogy VCF project was $170m. The cost of the written off work of Phases One and Two of Sentinel up to the firing of Lockheed Martin was $427m.

The total spend of these failed attempts to replace the ACS system was $597m and 10 years was wasted. The agile project, which is now delivering a solution, will only cost $114m for a three-year-long project.[41]

Questions

1. The original Trilogy program comprises three projects: a hardware upgrade, an infrastructure upgrade, and the development of the VCF case management facility. Of these three projects, which seems the most amenable to fixed-price tendering and which was the most likely to benefit from an agile approach?

2. A major criticism of the Trilogy VCF Project was that it was deficient in detailed monitoring of spend versus budget and that it lacked a detailed architecture before work started. These deficiencies were supposedly addressed at set-up for the subsequent Sentinel project. Were these deficiencies really of crucial significance in the failure of the Trilogy VCF project?

3. The FBI originally planned delivery of Sentinel in four overlapping phases. However, at the end of Phase One the start of the next phase was delayed to allow more time for detailed re-planning. Did this delay to plan in more detail reduce the risk of failure?

4. Because of the re-planning, a more incremental approach was agreed to the delivery of Phase Two in four segments. Due to technical difficulties, the implementation dates for these four segments were allowed to slip. Could the use of technical prototypes and practical targeted pilot usage have clarified the probability of success and the technical fault-lines at an earlier stage?

5. In 2010, the FBI decided to take on the risks of delivery from Lockheed Martin and manage the project directly using agile. Were overall risks actually increased by this bold step?

[1] {Perera 2012 #382}

[2] {OIG 2002 #289}

[3] {US OIG 2002 #288: xii –x /pageroman}

[4] {OIG 2011 #283: 7}

[5] {OIG 2006 #291: xi /pageroman}

[6] {Israel 2012 #383: 76}

[7] {OIG 2006 #291: ii–iii /pageroman}

[8] As stated in a memorandum of understanding (MOU) signed by the FBI, DOJ, and DHS CIOs in June 2005; see {OIG 2006 #291: 38}

[9] {OIG 2006 #291: iii /pageroman}

[10] {OIG 2006 #292: i /pageroman} and {FBI 2006 #286}

[11] {OIG 2006 #292: x /pageroman}

[12] {OIG 2007 #293: ix /pageroman}

[13] {OIG 2007 #293: i /pageroman}

[14] {OIG 2007 #293: vi /pageroman}

[15] {IBM Center for the Business of Government 2011 #399}

[16] {OIG 2008 #287: ix /pageroman}

[17] {OIG 2008 #287: 5}

[18] {FBI 2006 #286}

[19] {OIG 2009 #285: iii /pageroman}

[20] {Israel 2012 #383: 76}

[21] {FBI 2006 #286}

[22] {Israel 2012 #383: 78}

[23] {Israel 2012 #383: 75}

[24] {OIG 30/03/2010 #294: 2}

[25] {OIG 30/03/2010 #294: 8}

[26] {OIG 2010 #284: 4}

[27] {OIG 2010 #284: 5} and {OIG 2010 #284: 13}

[28] {OIG 2010 #284: 21}

[29] {FBI 2006 #286}

[30] {OIG 2011 #283: 1}

[31] {OIG 2011 #283: 25}

[32] {OIG 2011 #283: 24}

[33] {OIG 2011 #283: 19} and {OIG 2011 #283: 23}

[34] {OIG 2011 #283: Appendix I}

[35] {OIG 2011 #283: 17}

[36] {OIG 2011 #283: Appendix II}

[37] {MicroPact 2012 #296}

[38] {FBI CIO 2012 #324}

[39] {FBI CIO June 6, 2012 #371: 1}

[40] {FBI CIO June 2012 #372}

[41] {FBI CIO 2012 #405}