**RESEARCH REPORT**

## IT PROJECTS FAILURES & PROJECT PROCUREMENT ANALYSIS

## 

### A picture containing clipart Description automatically generated

by Daria Prianishnikova

BCIS207, Semester 1 2020, LGA

Contents

[Section 1. IT Project Failures 2](#_Toc38475765)

[Introduction 2](#_Toc38475766)

[Cases 2](#_Toc38475767)

[1. U.K.’s Nаtional Prоgramme fоr IT in the National Health Service 2](#_Toc38475768)

[2. Victoria Police Department’s LEAP Replacement Project 7](#_Toc38475769)

[3. Canadian Phoenix Pay System 9](#_Toc38475770)

[4. Massachusetts’s Department of Revenue Project 13](#_Toc38475771)

[5. California’s Unemployment Insurance Modernization Project 14](#_Toc38475772)

[6. U.S. Veterans Administration and Department of Defence’s Electronic Health Records System 16](#_Toc38475773)

[7. Chicago’s Project Shield 17](#_Toc38475774)

[8. U.K.’s FiReControl Project 18](#_Toc38475775)

[9. U.S. Secure Border Initiative Network 20](#_Toc38475776)

[10. BBC’s Digital Media Initiative 23](#_Toc38475777)

[Summary 27](#_Toc38475778)

[Section 2. Make or Buy Analysis 28](#_Toc38475779)

[Introduction 28](#_Toc38475780)

[Comparison 28](#_Toc38475781)

[Conclusion 30](#_Toc38475782)

[References 31](#_Toc38475783)

# Section 1. IT Project Failures

## Introduction

Major IT Projects are often subject to failure. They encounter crucial problems along the way and either end up being abandoned or inadequately delivered. Poor management, unsuited developing methodology, scope creeps, unrealistic budget and schedule are one of the many problems that lead to millions of money and years of development wasted.

As a current IT student and future IT professional, I will likely participate in IT projects myself. To be aware of mistakes made in other projects and learn from these mistakes, I am to research ten major IT project failures, investigate the reasons behind them, consequences they led to, and costs. Learning about these project failures can help raise awareness in the IT industry and avoid future mistakes

## Cases

### U.K.’s Nаtional Prоgramme fоr IT in the National Health Service

****Overview****

The Nаtional Prоgramme for IT in thе Nаtional Hеalth Service (or Connecting for Health) was a large-scale government IT project that took place in the United Kingdom (Campion-Awwad, Hayton, Smith, & Vuaran, 2014). NPfIT was launched in 2002 by Prime Minister Tony Blair, who wished to use technological possibilities of the 21st century to improve the NHS (Campion-Awwad, Hayton, Smith, & Vuaran, 2014).

Hospitals аnd GP Practices already had IT systems, but they were independent of one another, developed in-house or bought from various suppliers and customized to the individual organizations (Sampson, 2012). NPfIT, on the other hand, was intended to enable medical systems throughout the country to intercommunicate. This would be achieved by delivering the four key elements (Campion-Awwad, Hayton, Smith, & Vuaran, 2014):

* an intеgrаtеd electrоnic health records system
* online appointment bооking service
* cоmputerised rеferral and prescriptions systеms
* and nеtwоrk infrаstructure with enough capacity to support it.

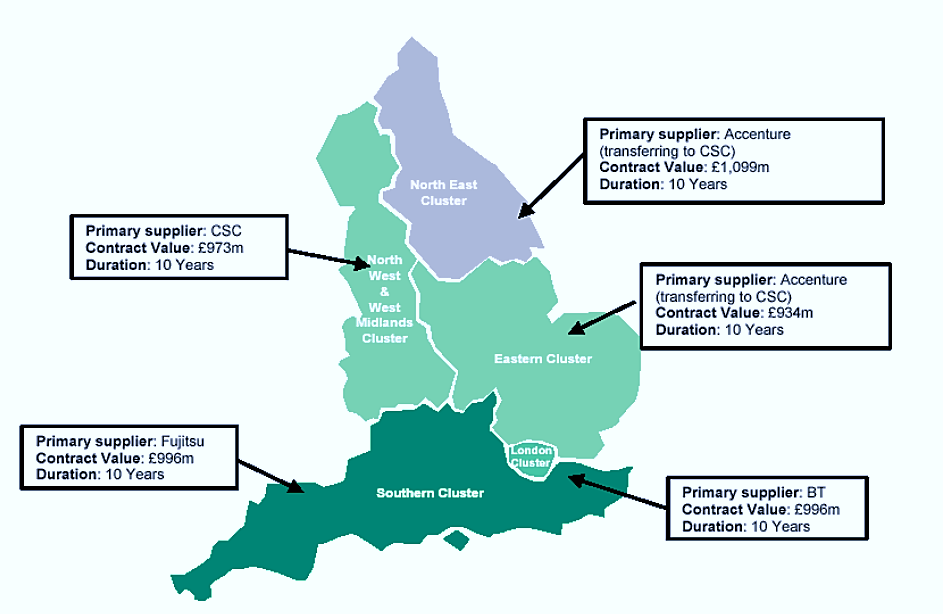
NHS estimated NPfIT would have to coordinate about six million patient visits to GPs, 13.7 million prescriptions, over three hundred thousand patient x-rays, and over 64.5 thousand emergency calls by ambulances (Sessions, 2008):

NPfIT’s budget was allocated in 2004 with an original number of around £6 billion over the lifetime of multiple major contracts (Lister, 2004). Those contracts were split over five geographical clusters, or regional group of health care providers and their patients (Sessions, 2008). Thus, NPfIT had at least a dozen contractors to deliver services to process over 300 transactions per second for 60 million people.

The following figures demonstrate the assignment of contractors to regional clusters and what services they would deliver:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Regional Cluster | | | | | |
|  | **North East** | **North West and West Midland** | **Eastern** | **London** | **Southern** |
| Primary Contractor | Accenture | Computer Sciences Corporation | Accenture | British Telecom | Fujitsu |
| Clinical Information Systems Contractor | iSoft | iSoft | iSoft | IDX | IDX |

**Figure 1: Primary and CIS contractors by regional cluster** (Sessions, 2008)



**Figure 2: Regional Clusters for Local Service Providers. Source:** (Committee of Public Accounts, 2013)

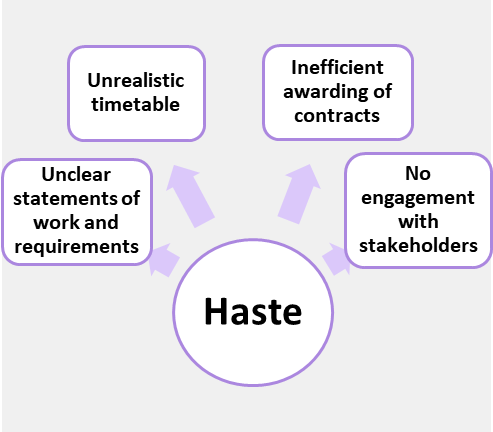
In September 2011, the British Government made an announcement that the NPfIT would be disassembled into its separate component parts with divided management and accountability structures (Committee of Public Accounts, 2013).

What went wrong?

There are many reasons which led to the project’s failure, often linked to one another, and can be grouped into three general categories (Campion-Awwad, Hayton, Smith, & Vuaran, 2014):

* **Haste**

The politicians and project managers rushed through policymaking, procurement and implementation processes of the programme. The Prime Minister Tony Blair asked for a very short time constraint of two years and nine months because of the upcoming general election in 2005 (Campion-Awwad, Hayton, Smith, & Vuaran, 2014). The tight schedule left little to no time for a consultation with the project’s key stakeholders about the decision to implement NPfIT.



**Figure 3: Results of haste in NPfIT** (Maughan, 2010)(Campion-Awwad, Hayton, Smith, & Vuaran, 2014)

Parliament was affected by the lack of consultation as well as it was not given enough time to contribute to the project’s plans like the procurement phase (Campion-Awwad, Hayton, Smith, & Vuaran, 2014). NPfIT hasted to award contracts without proper planning for such a large contract, making contract scope and deliverables unclear to the contractors (Maughan, 2010).

* **Poor design**

The Programme sought to replace tailored for specific hospitals ERP systems with one heavily centralized, nationwide system. Not only this approach did not fit with the needs of end-users, but it was given not enough consideration to how this would affect user satisfaction and confidentiality issues (Campion-Awwad, Hayton, Smith, & Vuaran, 2014).

Before the project was initiated, there had been concerns that centralised databases of healthcare information would be a target for corporations and government (Campion-Awwad, Hayton, Smith, & Vuaran, 2014). Yet the British Government still pursued with NPfIT disregarding those issues. During the implementation of Electronic Care Records, it was unclear what type of aggregated records would be shared or for what purpose. The public was not informed in detailed about what their information would be used for and who would receive the data. In addition, access concerns were raised regarding the potential abuse of staff access privileges and breach of data privacy (Campion-Awwad, Hayton, Smith, & Vuaran, 2014).

In the original implementation phase of NPfIT, there was no universal coding language, which made it a potential risk to patients’ safety. The overall implementation was executed poorly, which caused growing concerns about reliability. For example, in 2005 the software in the Summary Care Records Demographics Service malfunctioned and was shut down as it was incompatible with other versions of GP systems (Campion-Awwad, Hayton, Smith, & Vuaran, 2014). Many other healthcare professionals reported that the software was not fit for purpose and created potential risks as it would freeze and not save files or simply have the capability to record certain data (Campion-Awwad, Hayton, Smith, & Vuaran, 2014).

**Figure 4: Results of poor design** (Campion-Awwad, Hayton, Smith, & Vuaran, 2014)

* **Culture and Skills**

Another reason for NPfIT’s failure was the lack of clear directions, project management and an exit strategy, which could effectively deal with anticipated problems for this large project (Campion-Awwad, Hayton, Smith, & Vuaran, 2014).

It started with the wrong motives of ambitious politicians, who initiated the project for political reasons, rather than the right professionals who know about the issues involved (Maughan, 2010). The politicians ignored the government IT projects that had failed before NPfIT, mistreated concerns about confidentiality, and pushed for an unrealistic timetable.

Vendors had to deal with accepting one-sided contracts, inadequate negotiating and new requirements during delivery (Maughan, 2010). Alongside with the difficulty of delivering within the short timescales and high risks, several significant service providers have terminated their contracts.

Senior management constantly rotated, losing corporate knowledge and established, respected leadership, and accountability. The management involved in the project did not stop the project at the “right moment”, resulting in years and millions of pounds being wasted (Maughan, 2010).

**Figure 5: Results of Culture and Skills** (Campion-Awwad, Hayton, Smith, & Vuaran, 2014)

Costs

The budget of £6 billion that had been allocated in 2002 escalated over the years. The Government reported that costs of the programme was £7.3 billion to March 2012, and the estimated final costs would be £9.8 billion (Committee of Public Accounts, 2013). In 2013, it is reported to had cost £10 billion (Syal, 2013).

The final costs excluded any costs for Lorenzo care records system by CSC (£572 million) and legal disputes over the Department of Health terminating Fujitsu’s contract for care records system in the South of England in 2008 (Committee of Public Accounts, 2013).

### Victoria Police Department’s LEAP Replacement Project

Overview

Law Enforcement Assistance Program (LEAP) replacement project (some places referred to as LINK) for Victoria Police, Australia, was initiated in 2005 (State Services Authority, 2011). The core information system, rolled out in 1992, used by police to support operational policing was out-dated, inefficient, and expensive to run, so it required an update.

The Government allocated AU$50 million for the funding in July 2005, and a month later it was increased to $60.5 million due to the original number “not being enough”.



**Figure 6: LEAP Replacement Project Chronology** (State Services Authority, 2011)

In February 2006, thebusiness case was delivered. According to it, the replacement would meet the following requirements (State Services Authority, 2011):

* reduce crime rates and improve trust within community
* upgrade ethical management and data sensitivity skills in police
* gather better information and data
* streamline data entry
* improve security of police data and access.

In February 2009, a contract with Niche Technology was signed to deliver the off-the-shelf Niche Records Management System product, which had been successfully implemented by police in Australia and overseas (State Services Authority, 2011).

LINK was formally closed down in June 2011 after it ran into multiple problems regarding the budget, original business case and the choice of design for the new system (State Services Authority, 2011). It was instead replaced by a new project, Policing Information Management System (PIMS), based on the business case developed by KPMG, which, unsurprisinly, was abandoned in August the same year, existing only for a few months.

What went wrong?

* **Inadequate business case or scope creep**

Delivered in 2006 and written to fit the initial budget of only $60 million, the business case was the first factor that set the things into motion. The problems with business case, according to (State Services Authority, 2011), were:

* it did not contemplate whether the new system was a like-for-like replacement of leap
* the case didn’t address key issues
* the benefits outlined in it were broad, unmeasurable and unachievable
* did not state the major risk of integrating LEAP into the new systems and costs and difficulty involved in it
* unknown scope of the replacement project.

Most importantly, the business case was not updated at all during the project with new changes such as budget, schedule, scope, and etc.

* **“Like-for like” replacement decision**

As mentioned earlier, the business case did not state that the new system would be designed to be a like-for-like replacement of LEAP.

At some point, a decision to go for a custom like-for-like solution was made, choosing to reproduce all LEAP’s functionality (State Services Authority, 2011). This decision was conflicting with the business case and was not properly costed.

In addition, LEAP was designed in the 1970s with its many flaws and oudated but asked to be re-worked for modern policing. The “like-for-like” decison has compromised the Niche Technology product and prevented the potential improvements in business processes (State Services Authority, 2011).

* **Underestimated budget**

The project cost had been undervalued in the business case and was continuously underestimated throughout the project’s life (i.e. when the like-for-like decision was made) (State Services Authority, 2011).

In 2009, it was suggested that the project needed extra funding of $26.3 million from State Administered Unit (State Services Authority, 2011). However, approval was never granted.

When the project was closed, KPMG’s report indicated that the cost of completion would be close to $160 million. The project was $100 million short to be realistically completed (State Services Authority, 2011).

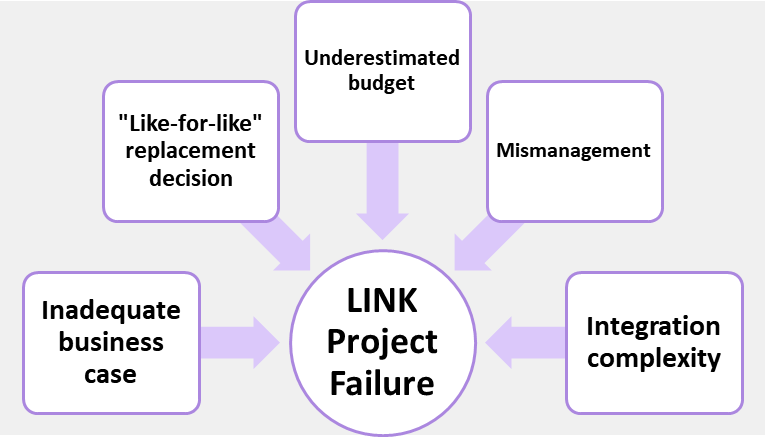
* **Integration complexity**

The integration of the old system with the new one was a difficult and time consuming task, as there were close to 200 interfaces with 25 existing applicatings that needed to be replaced (Herrick, 2011).

* **Mismanagement**

The (State Services Authority, 2011) “Inquiry into the LEAP replacement and other IT projects at Victoria Police” discovered that there was a lack of project management methodology and discipline leading to systemic mismanagement. SSA suggested that no one had the expertise to deliver major IT projects.

As for the LEAP replacement project, high staff turnover at Victoria Police and the lack of leadership at the time have contributed to mismanagement of the project.



**Figure 7: Reasons why LINK Project failed** (State Services Authority, 2011)

Costs

The (State Services Authority, 2011) report indicates that approximately $30 million has been spent since the project was initiated in 2006.

### Canadian Phoenix Pay System

Overview

In 2009, the Transformation of Pay Administration Initiative was started with Public Services and Procurement Canada undertaking two projects (Auditor General of Canada, 2018):

* one to centralize pay operations in Miramichi, New Brunswick, for 46 departments and agencies employing about 70% of all federal employees
* the other one to switch from the 40-year-old system to a new pay software system for all departments and agencies.

The Phoenix Pay System was completed in seven years with a budget of C$310 million, including $155 million to build and implement the new system (Auditor General of Canada, 2018). In short, the goals of the initiative were (Auditor General of Canada, 2018):

* centralize pay services
* decrease the costs of about $22 billion a year and improve the government’s payroll
* automate many pay processes
* integrate pay operations with the government of Canada’s HR management system to eliminate duplicate data entry
* eliminate 1,200 positions for pay advisors down to 550.

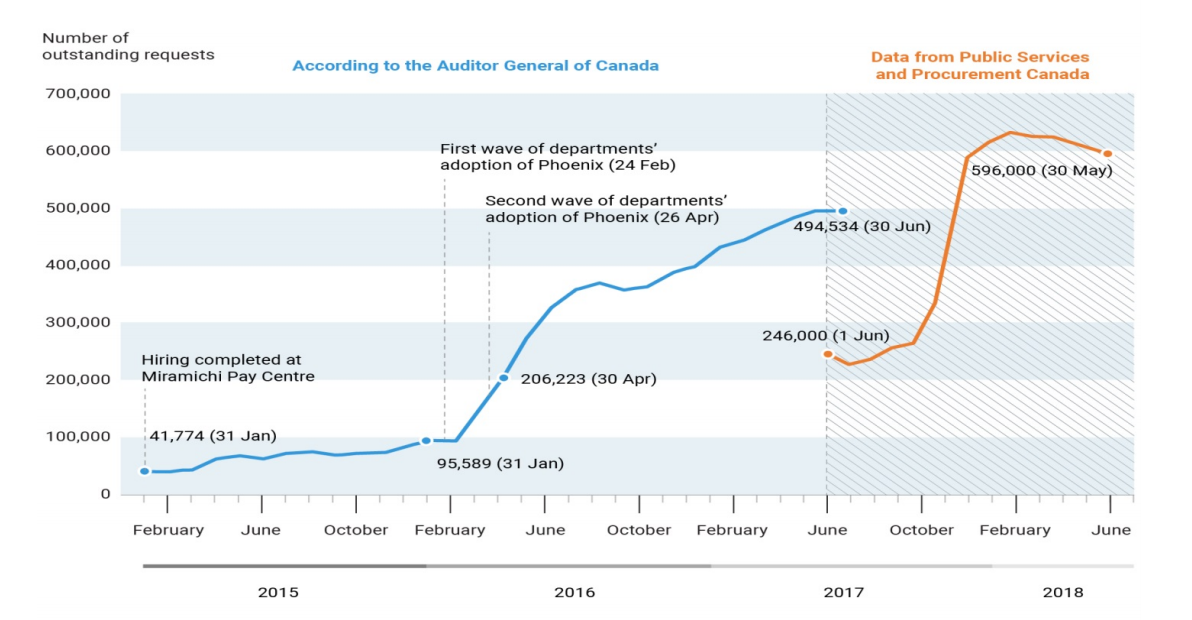
In June 2011, the Department hired IBM to help it design, customize, integrate and implement the off-the-shelf PeopleSoft software, which was called Phoenix (Standing Senate Committee on National Finance, 2018). Development began in 2012 and the implementation was planned in two stages, in October and December 2015 (Auditor General of Canada, 2018).

The implementation of Phoenix was complex as there were more than 80,000 pay rules and 200 custom-built programs to handle these rules and share information between Phoenix and HR systems needed to be included into the system (Auditor General of Canada, 2018).

IBM pushed the deadline for the launch to July and August 2016 based on the amount of work and changes that had to be done (Auditor General of Canada, 2018). Despite IBM’s warnings and Gartner’s recommendations that the software had not been fully tested and might cause payment delays, the Government proceeded with the first wave of implementation in February 2016, and the second wave in April 2016 (Auditor General of Canada, 2018).

Since Phoenix pay system was launched in February 2016, many problems became apparent (Auditor General of Canada, 2017):

* As of June 2017, the number of government public servants with an outstanding pay request had quadrupled to 152,517 and pay action requests had increased to 494,534 (see figure below for comparison with previous years)
* Employees had to wait an average of more than three months to have a pay request processed only two months after the system’s launch. By 2017, the waiting time increased to more than a year for nearly 49,000 employees
* By 2017, unresolved errors in pay outstanding totalled over $520 million.



**Figure 8: Number of outstanding pay action requests at the Public Service Pay Centre from January 2015 to May 2018. Source:** (Standing Senate Committee on National Finance, 2018)**, Figure 2**

As of 2020, Phoenix still operates, causing protests four years after launch (CBC News, 2020). It was announced that SAP won the competition with Ceridian and Workday to replace Phoenix and will test out their solution (CBC News, 2020).

What went wrong?

* **Project mismanagement**

Public Services and Procurement Canada decided to roll out a system that was not ready after their failure to manage it (Auditor General of Canada, 2018). Phoenix officials removed critical functions, cut back testing, and cancelled a pilot project so they would meet the project budget and timeline, (Auditor General of Canada, 2018). This resulted in the following (Auditor General of Canada, 2018):

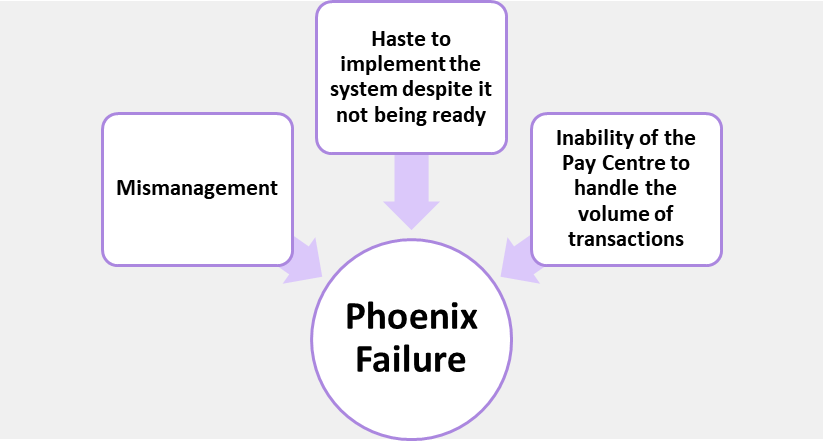
* Phoenix was implemented without critical pay processing functions and security measurements
* the system was not fully tested to see whether it was ready to be used government-wide
* it did not have any contingency plan in case the system had serious and systemic problems and any plans to upgrade the software application after it was no longer supported.

Additionally, Public Services and Procurement Canada did not fully consult and engage other departments and agencies during the development of Phoenix to determine its functionality (Auditor General of Canada, 2018). There was also no adequate help provided to those departments and agencies with the integration of Phoenix.

* **Unpreparedness for implementation**

The Phoenix officials looked over the fact that the Miramichi Pay Centre was not ready to handle the high volume of pay transactions (Auditor General of Canada, 2018). Departments and agencies were not prepared to move to the new system but forced to. Phoenix was not ready to correctly process the pay of employees (Auditor General of Canada, 2018). The decision by Phoenix officials to implement Phoenix was unreasonable, according to reports from consultants, IBM’s statements available at the time (Auditor General of Canada, 2018).

Also, there was lack of experience, expertise and training of the new 460 pay advisors at the Miramichi Pay Centre (Auditor General of Canada, 2018). Not many of the original 1,200 pay advisors who were eliminated agreed to work in Miramichi. Therefore, the Government had to hire many unexperienced employees (Auditor General of Canada, 2018).

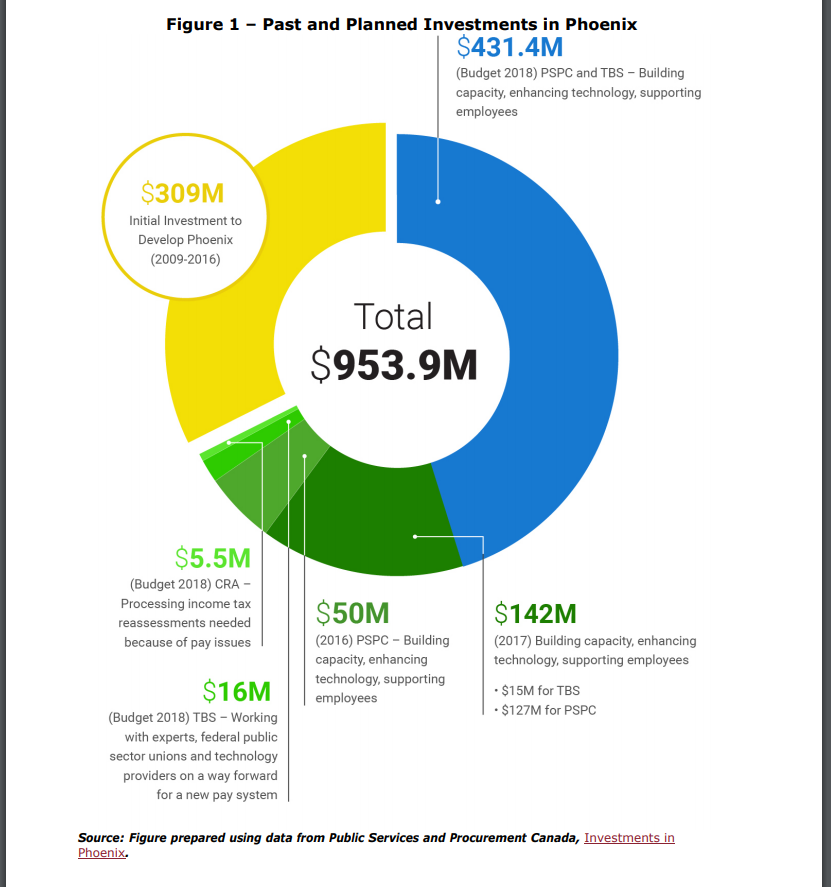


**Figure 9: Reasons why Phoenix failed**

Costs

The budget allocated in 2009 was $309 million, including the IBM contract, other professional services contracts and program costs.

After the system’s deployment and problems with it occurring, the government (or more like taxpayers) will suffer approximately $2.2 billion “loss” in investments to respond to pay issues over the seven-year period of 2016-2017 to 2022-2023 (Standing Senate Committee on National Finance, 2018). Total costs are better visualized in the following figure:



**Figure 10: Past and Future Investments in Phoenix. Source:** (Standing Senate Committee on National Finance, 2018) **Figure 1**

### Massachusetts’s Department of Revenue Project

Overview

In 2004, the Massachusetts Department of Revenue (DOR) considered development of a tax system, MASSTAX2, to integrate the full functionality scope of tax administration (Senate Committee on Post Audit and Oversight). The system’s goal was to improve tax collections, provide more personalized service to taxpayers, and enhance tax activities online (Woolhouse & Healy, 2013). In 2010, DOR signed a contract with Deloitte Consulting of New York for the MASSTAX2 project, and the work was initiated in January 2011.

Go-live date for the project’s initial deployment was March 2013, so a user-acceptance testing (UAT) commenced in September 2012 (Senate Committee on Post Audit and Oversight, 2014). UAT lasted 39 weeks and costed US$4.4 million instead of eight weeks and $1.8 million. UAT revealed more than 1,000 defects within the system (Senate Committee on Post Audit and Oversight, 2014). The issues were around the calculation of penalties and interest, notice printing and registration of taxpayers into the system (Kuranda, 2013).

Shortly after the UAT’s failure, the Department determined that the system would not go live and terminated the contract with Deloitte in August 2013. The Department found a new vendor to complete the project, a company called Fast Enterprises, and signed the contract in January 2014 (Senate Committee on Post Audit and Oversight, 2014).

What went wrong?

* **Miscommunication between parties**

Deloitte and DOR failed to communicate and work efficiently together to move the project forward on schedule and produce the working system (Senate Committee on Post Audit and Oversight, 2014).

* **The government’s decentralized organizational structure**

DOR’s organizational structure for the project was decentralized to provide the support, oversight and direction needed to ensure the successful delivery of the project (Senate Committee on Post Audit and Oversight, 2014).

* **Failed planning before and during the project**

The government client did not prepare a well-written business case. It did not fully document the reasons for the project, goals, risks and methods for mitigating them (Senate Committee on Post Audit and Oversight, 2014). Incorrect assumptions by both DOR and Deloitte led to the Oracle’s SAP program not being able to perform the calculation of penalties. In addition, problems in testing should have been anticipated (Senate Committee on Post Audit and Oversight, 2014).

**Figure 11: Reasons why MASSTAX2 failed**

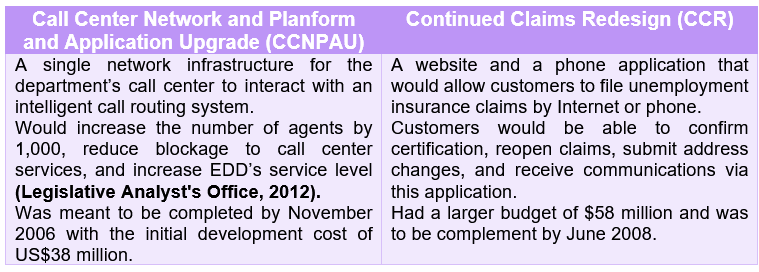
Costs

The budget for the project was $114 million but the contract with the vendor was terminated after paying $55 million (Senate Committee on Post Audit and Oversight, 2014).

### California’s Unemployment Insurance Modernization Project

Overview

In 2003, California’s Employment Development Department (EDD) planned two system developments that would help modernize its services (Charette & Romero):



**Figure 12: EDD's Unemployment Insurance Modernizations Projects in 2003**

Due to multiple independencies, the EDD proposed to combine the two projects in 2006, which required changing the scope, timetable, and costs of merged projects (Legislative Analyst's Office, 2012). Along with a single procurement, these changes brough the total costs of the project to $113 million and postponed completion by three years. CCNPAU would cost $48 million and completed by April 2010, CCR - $65 million and September 2011 (Legislative Analyst's Office, 2012).

EDD signed the contract with Deloitte Consulting to develop and implement the project. Throughout the years, estimated completion dates and costs kept changing but eventually the systems were rolled out. CCNPAU was completed in May 2011 and CCR was implemented in 2013 (Legislative Analyst's Office, 2012).

A week after EDD transitioned to its new unemployment system in the end of August 2013, technical problems began appearing (Charette, 2013). EDD reported that 185,000 (or 17%) of the nearly 800,000 Californians who receive unemployment benefits have been impacted by problems with the system before the error was fixed (Associated Press, 2013). At some point in September 2013, 124,000 people were waiting for their unemployment checks for weeks.

The issue was that the new systеm was misreading legacy data that was converted to the new system, causing delays in payments. The issue was fixed, and the system continued working but at the cost of $4 million on upgrading and fixing CCR (Charette & Romero).

What went wrong?

* **Errors during testing**

The errors fоund during unit tests in early system were not ever corrected and passed onto future builds of the system (Charette, 2013).

* **Data quality**

During the transition from a legacy system to its replacement it wasn’t ensured that existing data was clеan and complete so that it could be transferred into the new system without difficulties (Charette, 2013)

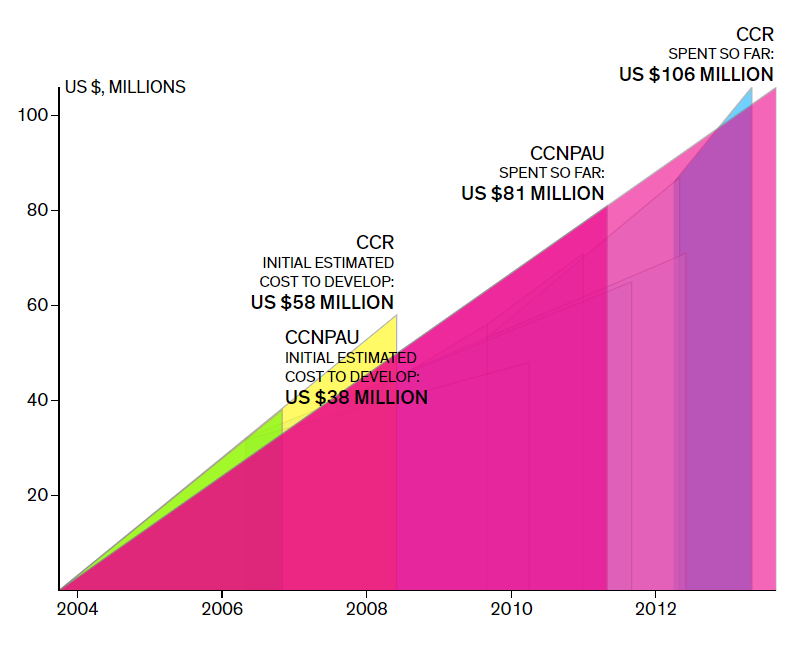
* **Vendor’s history of delays and failures**

Deloitte’s got a history of delays and problematic projects across California (and other states, i.e. Massachusetts’s Department of Revenue’s project in 2011-2013).

**Figure 14: Reasons for EDD closing the project**

Costs

The figure below shows the life cycle of the project with the projected costs per years. As of 2012, $106 million was spent on CCR and $81 million on CCNPAU, totalling in $187 million overall (Legislative Analyst's Office, 2012).



**Figure 15: The Life Cycle of the Project** (Charette & Romero, The Life Cycles of Failed Projects)

### U.S. Veterans Administration and Department of Defence’s Electronic Health Records System

Overview

In 2010, The Veterans Administrаtion (VA) and the Department of Defense (DOD) announced plans to begin the integration of their EHR systems, known as iEHR (Branz, 2013). iEHR would unify the two Department’s HER systems into a single system to ensure that all heath facilities have hеalth information available from both Departments (Panangala & Jansen, 2013).

The new iEHR would:

* promote transparency
* improve the quality of services through by reliable, complete, and accurate captured data
* imprоve interoperability between departments and enable medical data sharing
* support electronic medical data capture and exchange between the private U.S. health care system and the federal, state, and local government
* provide a quality, satisfactory patient experience
* reduce overall cost of health IT investments (Panangala & Jansen, 2013).

iEHR capabilities were to be achieved over a six-year period beginning in 2012 (Panangala & Jansen, 2013). The system would be based on Cerner’s Millennium software. The transition to the new iEHR was supposed to be completed by 2017.

However, on February 4, 2013, it was announced that iEHR required more work before it was ready to go live. Instead of building a single integrated system, it was decided to focus on integrating VA and DOD health data by using existing solutions (Panangala & Jansen, 2013).

What went wrong?

* **Scale of the project**

The goal of building a whole new HER for two departments from scratch and achieving interoperability was difficult, time-consuming, and expensive (Branz, 2013). DOR and VA were not prepared to make this goal come to life.

* **Mismanagement**

**Figure 16: Why iEHR failed**

Government Accountability Office blamed the iEHR integration failure on poor management, oversight, and accountability. This resulted in plans and time schedules lacking defined, measurable goals (Branz, 2013).

* **Top-down development**

The military has always built their systems top-down rather than bottom-up (Conn, 2013). This prevented end-user feedback and disconnected the two initial EHR systems.

Costs

The project was put on hold after four years and, most importantly, spending US$1 billion (Branz, 2013). I’ve found out that in 2019, according to (Mazmanian), more than $20 billion have been committed to the shared implementation of iEHR. DOD’s version of the Cerner system, MHS Genesis went live, but VA are set to begin adapting the system only in 2020.

### Chicago’s Project Shield

Overview

“Project Shield” was an IT government project for Chicago’s Cook County. It was meant to provide them with a capability to stream live video from dozen of fixed and mobile video surveillance cameras throughout the Chicago region to wireless-equipped first responder vehicles or 128 municipalities in case of emergencies (Charette, 2012). The project was initiated in 2003 in response to 9/11 attacks. It was scheduled to be completed in 2008 at a budget of US$31 million (Charette, 2012).

In October 2004, the Cook County Board of Commissioners selected 128 municipalities (mainly police departments but also some fire and emergency management personnel) for the installation of “Project Shield” equipment (Office of Inspector General, 2011). Those municipalities were to receive two vehicle systems, a hot spot, and a tower camera (Office of Inspector General, 2011). The installation was scheduled to be completed in several phases.

The Phase 1 contract was awarded in October 2004 for $12.8 million to install systems in 27 municipalities (Office of Inspector General, 2011). The Phase 2 contract was awarded in November 2005 for $11.3 million to establish systems for an additional 20 municipalities (Office of Inspector General, 2011). Installations continued from March 2005 until June 2006. Not long after the vehicle video systems were installed, the municipalities started to experience problems with equipment, so the vehicle installations were stopped (Office of Inspector General, 2011).

In 2007, the county decided to terminate the Phase 1 and 2 contractors after spending $23 million (Office of Inspector General, 2011). In May 2008, the country awarded a Phase 3 contract to a new contractor for $10.9 million to install at se municipalities and repair existing equipment (Office of Inspector General, 2011).

In April 2011, “Project Shield” equipment was installed in 87 out of 128 municipalities, which still were experiencing equipment problems and training issues (Charette, 2012). In July 2011, the County officials closed the project (Office of Inspector General, 2011).

What went wrong?

* **Lack of testing and planning**

Cook County did not test the equipment for “Project Shield” properly in different weather conditions, locations, and for integration with existing equipment (Office of Inspector General, 2011).

Equipment at the municipalities was not always located in the best spots, and the “Project Shield” software would not integrate with existing communications equipment and/or was not compatible with municipalities’ central dispatch systems (Office of Inspector General, 2011).

County officials claimed that the project had been initiated at a time when funds had not been available to perform planning in order to reduce the technical uncertainties (Office of Inspector General, 2011).

* **Mismanagement**

Cook County was unable to guarantee to the municipalities that they could operate the equipment as expected because the equipment was not working or the personnel lacked training to operate it (Office of Inspector General, 2011).

In addition, the county did not always comply with procurement, property, and record requirements. (Office of Inspector General, 2011) suggested that the federal funds were not spent effectively by finding missing records, issues with procurement practices, and unallowable costs.

**Figure 17: Why "Project Shield" failed**

Costs

Between the years of 2003 and 2009, Cook County spent about $45 million in federal funds for the installation and maintenance of “Project Shield” equipment (Office of Inspector General, 2011).

### U.K.’s FiReControl Project

Overview

FiReControl was a part of the “Fire and Resilience Programme” and aimed to improve the Fire and Rescue Service (National Audit Office, 2011). This was to be achieved by (National Audit Office, 2011):

* Building a network of nine purpose-built regional control centres instead of 46 local control rooms
* using a national IT system for calls handling, equipment mobilisation and managing incidents
* supporting Fire and Rescue Service’s business change by preparing each Service for new operational processes and policies, staffing and ways of working

Initiated in 2004, FiReControl was scheduled to be completed by October 2009 with the budget of £120 million (National Audit Office, 2011). In 2007, the Department for Communities and Local Government contracted European Air and Defence Systems (EADS or now known as Cassidian) to design, develop and install the computer system for the project (National Audit Office, 2011).

The project was subject to delays, escalating the costs to finish the project to £635 million, (National Audit Office, 2011). In June 2010, The Department assessed the deliverability of FiReControl and concluded that it was uncertain whether the delivered system would be adequate, or would it be worth the time and cost to achieve it (National Audit Office, 2011).

The Department for Communities and Local Government determined that the project could not be delivered within an adequate schedule and it was decided to cancel the project altogether in December 2010 to avoid future costs and terminate the contract with EADS (National Audit Office, 2011).

What went wrong?

* **Insufficient communication and engagement with stakeholders**

Insufficient communication and engagement with local Fire and Rescue Authorities and their Fire and Rescue Services during the initiation and design of the project rose concerns about the regionalisation and the lack of clarity on how a regional approach would help increase efficiency (National Audit Office, 2011).

* **Stakeholders were not encouraged to support the delivery of the project**

As the result of the Department failing to communicate with local Fire and Rescue Authorities, they were not encouraged to support the delivery of the project (National Audit Office, 2011). Accountability for delivery was not placed in the hands of the Fire and Rescue Authorities (they were not legally obliged to use the system after its completion) who had the authority to commit the resources and accept operational responsibility (National Audit Office, 2011).

* **Underestimated complexity**

The Department underestimated the complexity of designing a system to meet the needs of Fire and Rescue (National Audit Office, 2011). In order to accommodate the wide variation in operational needs of the Services, key components required significant modification (National Audit Office, 2011). The Department made EADS responsible for achieving the required standardisation to without providing them proper user requirements (National Audit Office, 2011).

* **Unrealistic estimates of project costs and timetable**

The Department and Treasury dedicated to the project based on unrealistic estimates of costs of £120 million (National Audit Office, 2011). Those estimates did not include the costs of installing equipment or meeting local and regional implementation, so when the Department assessed costs and savings in 2007, estimated project costs increased to £340 million (National Audit Office, 2011).

* **Mismanagement**

In 2008, it was concluded by the Office of Government Commerce that the project board was not operation as an effective decision-making forum (National Audit Office, 2011). Despite the Department’s attempts to strengthen its governance arrangements in 2009, it was “too late” to correct earlier problems (National Audit Office, 2011).

* **Lack of leadership and high staff turnover**

The project had a high turnover of staff, over-reliance on poorly managed consultants, and inconsistent leadership (National Audit Office, 2011). There have been five different Senior Responsible Owners, four different Project Directors and five officers supervising the delivery of the project (National Audit Office, 2011).

* **Miscommunication between the contractor and the agency**

The Department failed to ensure that EADS followed the contracted approach in developing the system when having problems with integration of sub-systems (National Audit Office, 2011). The miscommunication between both parties towards problem solving led to the slow resolution of issues (National Audit Office, 2011).

In addition, the EADS’s contract stated that they would be paid only once a key milestone for the building and testing of the system had been passed (National Audit Office, 2011). The delays to delivery led to cash flow difficulties for EADS, creating further misunderstandings with the Department.

**Figure 18: Why FiReControl failed**

Costs

By the end of March 2011, £250 million have been spent in total on the project and the minimum that would be wasted as a result of the failure to deliver the project would be £469 million (National Audit Office, 2011).

### U.S. Secure Border Initiative Network

Overview

Secure Border Initiative Network (SBInet) was launched in 2005 by U.S. Customs and Border Protection (CBP) (Government Accountability Office, 2010). The purpose of the project was to create a “virtual fence” by combining surveillance technologies that replied on radar and camera towers along the southwest border in order to secure it from contraband and prevent illegal immigration (Government Accountability Office, 2010). The prime contract for the project was awarded to Boeing Corporation in September 2006 (Department of Homeland Security, 2011).

SBInet’s initial and only deployment, known as Block 1, was deployed in 2010 to 53 miles of the Arizona border (Government Accountability Office, 2010). The deployment included nine mobile towers, cameras, radars, vehicles with laptops, and satellite phones or handheld devices (Hsu, 2008).

Since its launch, SBInet had technical problems, cost overruns, and schedule delays (Government Accountability Office, 2010). In 2011, after concerns stated in internal and external assessments regarding the performance of the project, cost, and schedule for implementing the systems, further procurements of SBInet systems were cancelled (Government Accountability Office, 2010). CBP, however, planned to continue to operate the existing systems and implement a successor, the Arizona Border Surveillance Technology Plan, to cover the remaining area of the border (Department of Homeland Security, 2011).

What went wrong?

* **Haste**

After 9/11 attacks and immigration report, the government rushed to show the American public that the government was fulfilling its responsibility to secure the border (Why SBINet has failed, 2010). The haste led to the government not doing an adequate job in preparing for the project.

* **Continuous change**

Since the program began, important aspects such as scope and timing of deployments, testing methods of SBInet were continuously changing, making it unclear what technology capabilities were to be delivered when (Government Accountability Office, 2010).

* **Unclear requirements**

SBInet requirements had not been effectively defined and managed (Government Accountability Office, 2010). Boeing, the primary contractor for the project, was largely on its own. The government did not provide the guidelines of what kind of program platform and technology they wanted and did not work closely with Boeing to develop it (Why SBINet has failed, 2010).

* **Ineffective testing**

The program office did not test the individual system components, even though the contractor initiated integration testing (Government Accountability Office, 2010). Furthermore, the project’s test management strategy did not contain detailed information for specific test events or a clearly defined testing roles and responsibilities (Government Accountability Office, 2010).

* **Off-the-shelf software**

For the integration of data related to illegal border-crossing, Boeing used off-the-shelf commercial software designed for police instead of military-style one (Hsu, 2008). This software could not deal with large amounts of sensor data, preventing operators in a command center from locking cameras on targets (Hsu, 2008).

* **“One size fits all”**

The SBInet system is not the best and most cost-effective system for all areas of the border (due to terrace, population differences, etc) and does not have the capability to provide a “one size fits all” integrated solution to secure the border (Why SBINet has failed, 2010).

* **Mismanagement**

Overall, the Department of Homeland Security was not able to provide effective management over the project and its primary contractor (Government Accountability Office, 2010). DHS did not fully define activities, milestones, and costs for implementing the program and kept changing them over the life of the project (Government Accountability Office, 2010). DHS also did not effectively provide oversight and management over the contractor, not knowing whether the contractor is meeting performance and product expectations (Government Accountability Office, 2010).

**Figure 19: Reasons for the failure of SBInet**

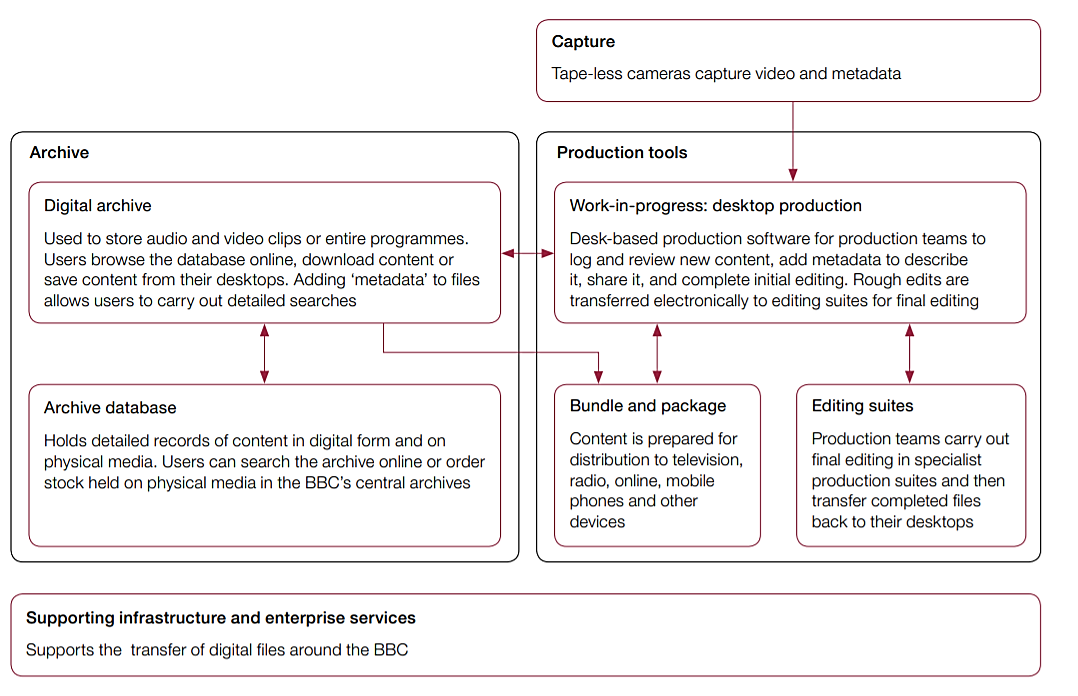
Costs

The only deployment of the SBInet program (two regions in Arizona, covering 53 miles out of 387-mile border with Mexico) has cost nearly $1 billion (Department of Homeland Security, 2011).

### BBC’s Digital Media Initiative

Overview

The Digital Media Initiative, established in 2006, was a business transformation programme to allow BBC staff and partners to develop, create, share and manage video and audio content and programming on their desktops (National Audit Office, 2014). To achieve that, BBC decided to build a custom-made digital system that consisted of:



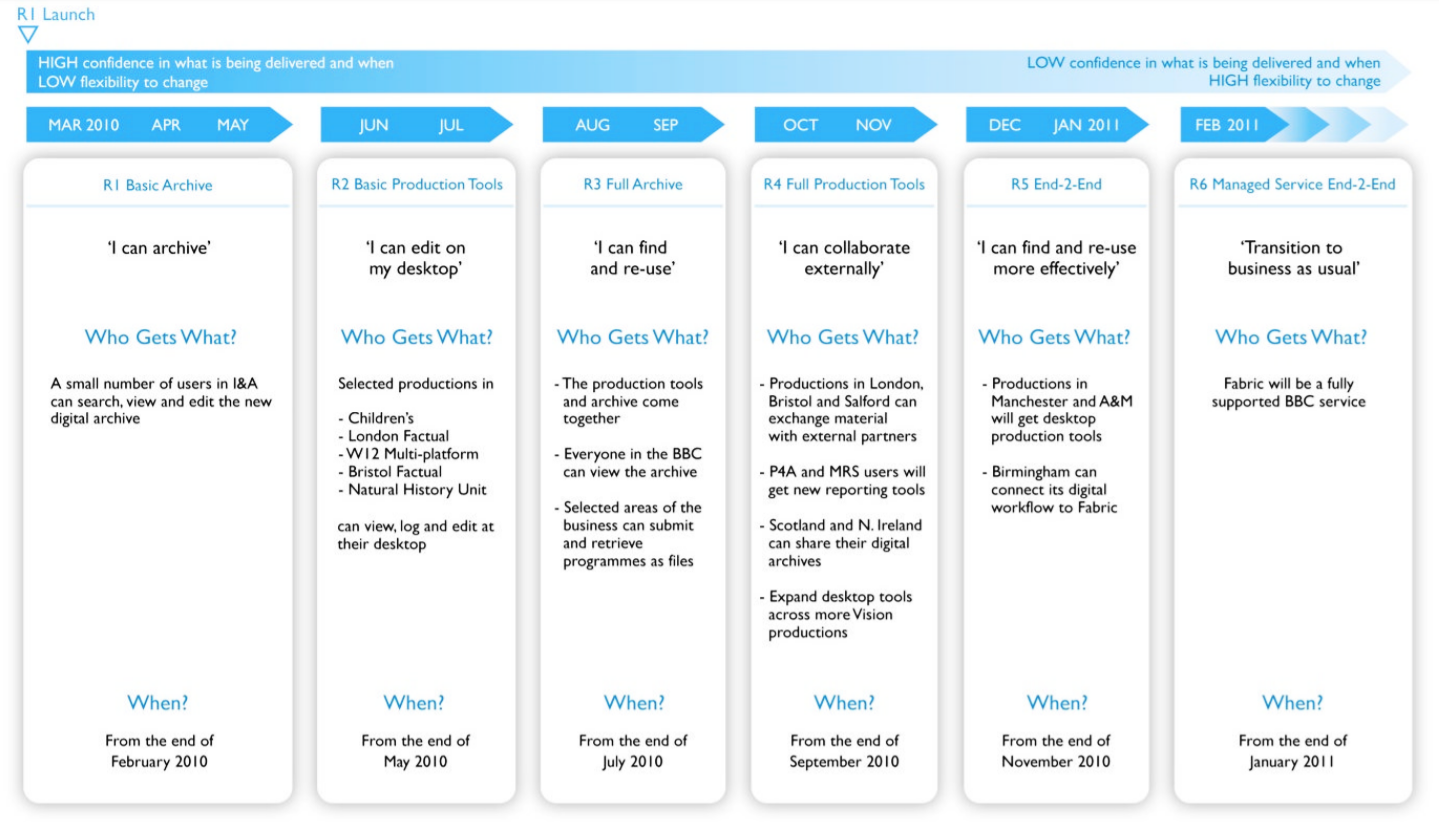
**Figure 20: Original concept for how the DMI system would work. Source: Figure 1** (National Audit Office, 2014)

The BBC contracted Siemens to build the system in February 2008 (PwC, 2013). The fixed price contract established a plan that the project would be completed in 18 months at a cost of £79 million (British Broadcasting Corporation). The contract was mutually terminated in July 2009 after numerous delivery delays (PwC, 2013).

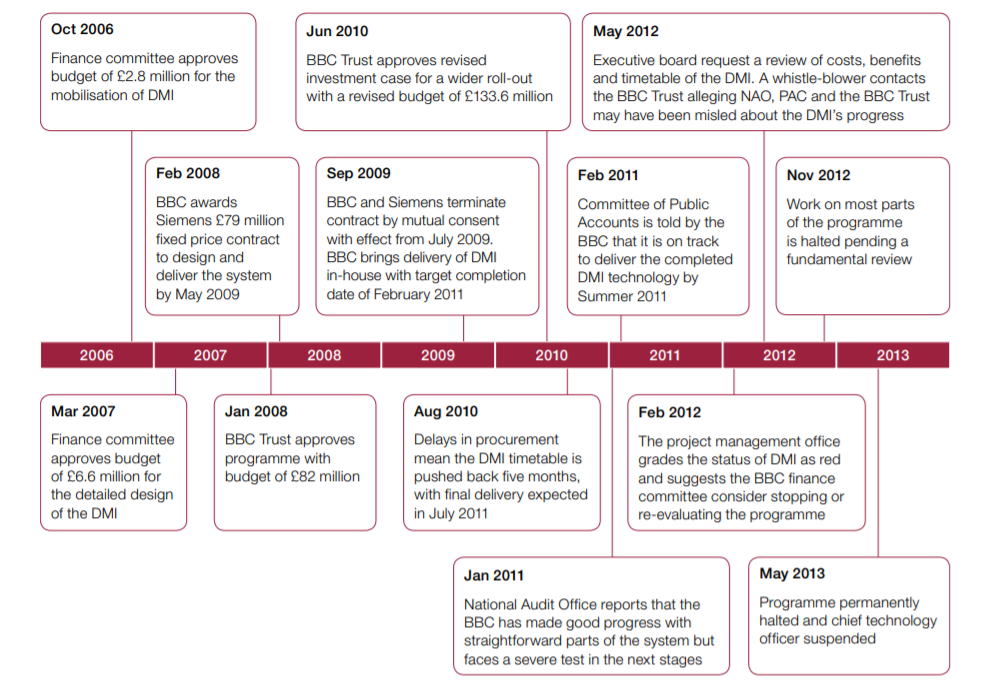
The BBC took the system’s implementation in-house from September 2009 (National Audit Office, 2014). The BBC considered that it could make up the capability by recruiting experienced staff or using third-parties suppliers to build system components that the BBC would later integrate (National Audit Office, 2014).

After numerous delays, inability to deliver a working system, internal and external reports, the BBC decided to close the rest of the DMI project in May 2013 but keep maintaining the archive database (National Audit Office, 2014).

The figures below are the original timeline presented in 2010 for each release and the timeline of what happened with the project. DMI recognised that a high degree of confidence as to what would be delivered in the initial phases would reduce over time because business requirements could change (PwC, 2013).



**Figure 21: BBC DMI scope and timeline presented in March 2010. Source: Figure 2** (PwC, 2013)



**Figure 22: Summary of events. Source: Figure 4** (National Audit Office, 2014)

What went wrong?

* **High risks of developing in-house**

The BBC’s decision to take the DMI in-house was high-risk as it needed to fill capability gasps to deliver DMI components and meet important internal deadlines (National Audit Office, 2014).

* **Mismanagement, lack of accountability**

The BBC did not appoint a senior responsible owner of the project who would be accountable and bring together all elements of the project (National Audit Office, 2014). The absence of a senior responsible owner led to unresolved issues between divisions that develop the system and its intended users.

Key leadership roles in the DMI, including the programme director and technical director, changed several times, creating a gap in knowledge of the project (National Audit Office, 2014).

* **No transparent reporting**

Clear, transparent and consistent reporting was not provided in the DMI, despite the business case stating so (National Audit Office, 2014). Reporting was supposed to be on progress against plan, cost to complete, or delivery of benefits to enable effective decision-making (PwC, 2013). In addition, reporting on a quarterly basis (as that is how long it took to deliver the report) resulted in the reported status of DMI being behind the current status (National Audit Office, 2014).

* **Confusion with release schedule**

The DMI was planned to be implemented in phases by releasing a series of technology adding new capabilities. However, the BBC changed its technology release plans due to technical and timetabling issues and created confusion about what each release was supposed to provide (National Audit Office, 2014).

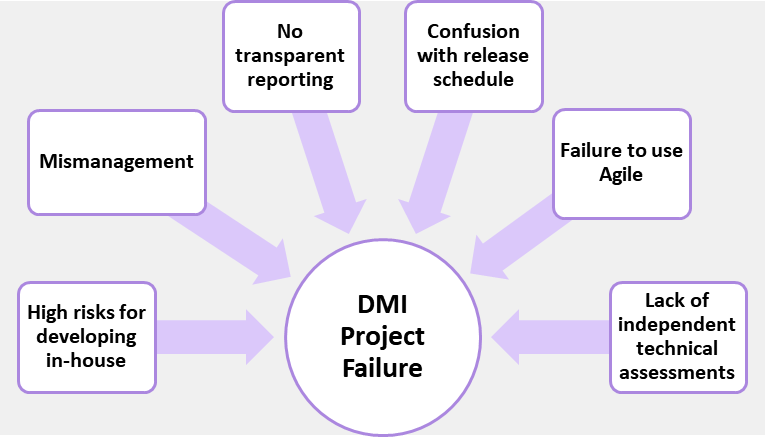
* **Failure to use Agile and poor engagement with the users**

The project was to be delivered using Agile development methods (Glick, 2014). Nevertheless, the business refused to work closely with the development team and instead waited for the full functionality of large incremental pieces. As a result of scrapping agile, the users kept changing requirements (like first wanting an in-house developed product but then refusing to use it and asking for an off-the-shelf product from Adobe instead) and never fully understood the scale of changes required and adding additional work for the IT team and causing delays in delivery (Glick, 2014).

* **Lack of independent technical assessments**

The BBC did not ensure that the DMI’s technical designs can be implemented by ordering an independent technical assessment of the system design when it appointed Siemens or when it brought the DMI in-house (National Audit Office, 2014)

There was one draft of an assessment done by Accenture in December 2010, which covered two specific areas of the system (National Audit Office, 2014). Even then, Accenture found that a significant amount of correction was required in system infrastructure for the DMI for producing television content (National Audit Office, 2014).

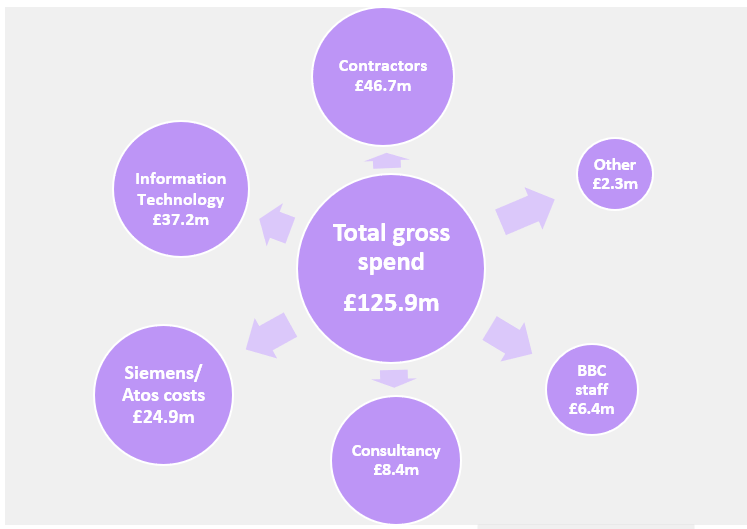


**Figure 23: Reasons for the failure of the Digital Media Initiative Project**

Costs

The BBC spent £125.9 million (gross) on the DMI from April 2007 to September 2013 (National Audit Office, 2014). The following figure breaks down the cost into areas with amounts spent on them:

**Figure 24: Where the money went. Source: Figure 9** (National Audit Office, 2014)



## Summary

The most common reasons for the failures of the ten researched projects are mismanagement, underestimated costs, timetable, and scale of the project. I believe this is connected to nine out of ten projects being government IT projects. There is a common trait – most of them are all delivered top-down, with government agencies having ambitious, unrealistic expectations that they pass on to developers. However, the government agencies in most cases do not have the expertise or the experience to manage those large-scale projects, often leading them without proper guidance or accountability for millions of dollars or pounds spent.

Scope creep is another good reason for some of the project failures. NPfIT’s requirements were not properly defined; Victoria Police Department’s LEAP’s business case was not updated at all with a new scope; Massachusetts’s Department of Revenue, too, did not prepare a well-written, detailed business case; Secure Border Initiative Network was subject to continuous change throughout the project’s life; BBC’s Digital Media Initiative’s users kept changing the requirements after the developers’ team completed their previous requests. These projects show how important it is, for both the management and potential users, to know how to prevent scope creep.

It is hard to tell if any of the project failures may have been related to the wrong choice of development methodology as the researched information did not mention any development methodologies. Only one project, the BBC’s Digital Media Initiative, disclosed what methodology they were going for, which was Agile. Even so, the business side of the project failed to follow the Agile principle of working closely and daily with the developers, resulting in constant pushbacks.

As for the remaining nine projects, I can only assume what methodology may have been the best for some of them, based on the reasons why those projects failed. NPfIT would be another good candidate for the use of Agile, as one of the reasons for the project’s failure was “not enough engagement with stakeholders”. The developers’ team did not examine the needs of the users thoroughly, making software that the medical professionals were not keen to use. With Victoria Police Department’s LEAP Replacement Project, there were too many risks involved in integrating a legacy system with a newly developed one. Perhaps, if a Spiral Model methodology had been used, it would have analysed those risks and prepared for them.

All these project failures can teach developers and, mainly, government bodies many valuable lessons on how to successfully deliver major IT projects. Personally, the main lesson for me was that it is very important to work closely with the business side of the project. Getting clear requirements from them and ongoing feedback from the users is vital for the successful delivery of a project. It would reduce future miscommunication with the management, help build a system that meets the users’ needs, and avoid scope creep.

# Section 2. Make or Buy Analysis

## Introduction

A decision to introduce a new software product to meet the company’s needs can be challenging. On one hand, there is an off-the-shelf product that can be simply purchased for a cheaper price and enhanced to get the missing capability. On the other hand, there is a custom solution can be built at a higher price and in a longer time period. The custom solution will have all the functionality a business needs or will need in the future for its growth.

As the IT Manager of a company that is trying to choose between buying or building in-house a new inventory management program, my goal is to research what cases and\or factors can help make the right decision.

There are many risks and steps involved in switching to new software alone whether it’s bought or custom-made. Making the right choice for a specific case can prevent the company from wasting large amounts of resources such as time and money beforehand.

Based on the findings that investigate the differences between the two choices in key factors, I will express my concerns and make recommendations that may be potentially used in the further decision making.

## Comparison

Resources

The very first and most important factor in deciding whether to buy or make a program is **price**. For custom software, there is a significant upfront cost. If the budget is small, it is logical for a business to avoid building custom software. Commercial off-the-shelf solutions are cheaper but the cost may grow over time and in most cases software licences are limited to a time period or a certain number of users (Cohn, 2014).

Secondly, it comes to the **time** of completion. Developing software is a complex and long process. If a business does not have the time to successfully complete the project, it is best to think about buying rather than building (Cohn, 2014).

Thirdly, in order to develop software from scratch or even modify and implement a purchased solution, a company needs **workforce**. A skilled, technically proficient team is required for software development and the team will be accountable for a successful delivery of the project from start to finish (Cohn, 2014). If a company does not have one or cannot divert staff from one project to the development of custom software, it will be challenging to create an adequate product (Cohn, 2014). If there are no options but to build an application, build a small straightforward software that can be handled quickly by a small team of developers (Ulfelder, 2003). Another solution would be outsourcing applications development if a business must develop its own applications (Fields, 1995).

Capability

Off-the-shelf software cannot provide with all the functionality to meet every required need (Cohn, 2014). Nevertheless, there are many major solutions available that have proven to be effective , so they are worth buying rather than “reinventing the wheel” (Ulfelder, 2003).

If a business has specific needs, custom software may be a better choice to meet them, as it’s specifically designed from customer’s requirements (Cohn, 2014). Custom software will include all the functionality, operate the way a business wants it to, and allow flexible scalability of features or number of users (Yurevich, 2019).

However, if there are several available cloud or off-the-shelf products that cover 80% or more of requirements, then a business should consider buying (Doig, 2015). If it’s less than 60%, then there are some possibilities to approach off-the-shelf products (unless neither of them work well enough, then it’s back to building the software) (Doig, 2015):

* reduce the scope of the project by cutting certain functionality
* combine two or more commercial products
* combine a bought product with a customized module.

Some software, at least from large companies, has closed-source code, meaning it does not allow its code to be modified. It can be difficult to find an off-the-shelf solution that does allow to add or subtract built-in features (Cohn, 2014). If the need to buy a software arose, it is best to look for a highly customizable, packaged software or look into open-source software (Fields, 1995). The so-called off-the-open-sourceshelf software has become a wide-spread phenomenon and opened up new possibilities, saving hundreds of hours of development time and a lot of money (Kent, 2006).

Integration

Custom solutions are built so they can integrate with any existing software, tools, and processes that a company already uses (Yurevich, 2019).

Purchased software, on the other hand, may not be compatible with other programs in use and decrease efficiency if not working with other programs smoothly (Cohn, 2014). To ease the integration process, it is recommended to buy multiple applications from one vendor (Ulfelder, 2003)

Control

Control over a software solution would include updates, security measures, decisions on future features, etc.

As the owner of an in-house built program, a company will be completely in charge for all those decisions and be able to release the product to the market and make profit (Yurevich, 2019).

With off-the-shelf software, it’s the vendor who controls updates, functionalities, and volume capacity and makes all the key decisions on the software’s future (Yurevich, 2019). However, as third-party vendors want to stay completive and not lose customers, they will regularly update the software and can maintain it (Yurevich, 2019).

Competitiveness

Custom-built program can provide a business with a competitive advantage over others by increasing performance, scalability, and productivity (Cohn, 2014). If a custom-built application is needed to differentiate a business from competitors, it is worth building it (Ulfelder, 2003).

But that is not always the case, as if a business is “generic” like a retail furniture store, then it does not need a brand new custom software as it would unlikely benefit the company’s competitiveness or provide a higher quality service or lower prices (Cohn, 2014).

## Conclusion

|  |  |  |
| --- | --- | --- |
| **Things to consider** | **Custom Software** | **Off-the-shelf software** |
| Can it meet **every** need of a company? | Yes | No |
| Can it be modified? | Yes | Not always |
| Will it be compatible with existing software? | Yes | Not always |
| Price | Expensive | Cheap |
| Do you need a team of highly skilled software developers? | Yes (unless outsourcing) | Not necessarily |
| Time taken | Long | Fast |
| Is it be needed to give a technological advantage over competitors? | Yes | No |
| Is it proven to be effective for a common organization’s purpose? | Not always | Yes |
| The organisation of users’ workflow | Can be a single integrated platform that allows higher productivity | Can be multiple different programs that users will have to switch between |
| Is it a good investment for a long-term use? | Yes | Not always |
| Is it easy to scale software to a company’s size? | Yes | Not always |

The following table summarizes the findings and contains some of the factors that need to be considered when deciding:

Table 1: Summary of findings on Buy vs. Build Decision

**My recommendations and concerns are the following:**

After conducting a list of requirements for the company’s new inventory management system, we must investigate available solutions on the software market. If there are off-the-shelf solutions that cover more than 80% of the requirements for our inventory management system, it would be cheaper, faster, and more efficient to purchase it. This way, we will greatly reduce the costs and time, and will not have to divert staff from other projects or outsource the development. However, we must ensure that it comes from a reliable vendor, can be easily integrated with our existing system, and is highly customizable. If there are solutions that cover 60% and less, we can either:

* reduce the scope of functionalities
* look at combining multiple applications to make up for the lack of capabilities
* our IT team can create a customized module or tweak the software if it is possible.

Another option would be looking into open-source software. This will guarantee the ability to add the missing functionalities ourselves.

If buying or using an open-source software are not possible for any reason, then, if the project is feasible, we can consider developing in-house or outsource the development. For the in-house development, we need to make sure our team has the appropriate skillset to successfully finish the development and is available to make the new inventory management system a priority over other on-going or future projects.

# References

Associated Press. (2013, September 21). *Unemployment checks delayed by California EDD computer problems*. Retrieved March 27, 2020, from Los Angeles Daily News: https://www.dailynews.com/2013/09/21/unemployment-checks-delayed-by-california-edd-computer-problems/

Auditor General of Canada. (2017). *Phoenix Pay Problems.* Ottawa. Retrieved March 23, 2020, from http://www.oag-bvg.gc.ca/internet/English/parl\_oag\_201711\_01\_e\_42666.html

Auditor General of Canada. (2018). *Building and Implementing the Phoenix Pay System.* Ottawa. Retrieved March 23, 2020, from http://www.oag-bvg.gc.ca/internet/English/parl\_oag\_201805\_01\_e\_43033.html

Branz, K. (2013, June 14). *After 4 Years and $1 Billion, the VA and DoD Abandon Plans for a Fully Integrated EHR*. Retrieved March 28, 2020, from Dark Daily: https://www.darkdaily.com/after-4-years-and-1-billion-the-va-and-dod-abandon-plans-for-a-fully-integrated-ehr-614/

*British Broadcasting Corporation*. (n.d.). Retrieved April 14, 2020, from Why do project fail?: http://calleam.com/WTPF/?p=5998

Campion-Awwad, O., Hayton, A., Smith, L., & Vuaran, M. (2014). *The National Programme for IT in the NHS: A Case History.* University of Cambridge. Retrieved March 14, 2020, from https://www.cl.cam.ac.uk/~rja14/Papers/npfit-mpp-2014-case-history.pdf

CBC News. (2020, March 6). *Phoenix replacement chosen for testing*. Retrieved March 23, 2020, from CBC: https://www.cbc.ca/news/canada/ottawa/phoenix-pay-system-replacement-sap-1.5488435

CBC News. (2020, February 29). *Public employees protest Phoenix pay system*. Retrieved March 23, 2020, from CBC: https://www.cbc.ca/player/play/1704104515988

Charette, R. (2012, January 12). *Chicago Project Shield's Depressing Post Mortem*. Retrieved April 3, 2020, from IEEE Spectrum: https://spectrum.ieee.org/riskfactor/computing/it/chicago-project-shields-depressing-post-mortem

Charette, R. (2013, October 17). *California’s EDD Unemployment System Disaster: Predictable Fiasco?* Retrieved March 27, 2020, from IEEE Spectrum: https://spectrum.ieee.org/riskfactor/computing/it/californias-edd-unemployment-system-disaster-predicted-fiasco

Charette, R., & Romero, J. (n.d.). *The Life Cycles of Failed Projects*. Retrieved March 27, 2020, from IEEE Spectrum: https://spectrum.ieee.org/static/the-life-cycles-of-failed-projects

Cohn, C. (2014, September 14). *Build vs. Buy: How to Know When You Should Build Custom Software Over Canned Solutions*. Retrieved April 20, 2020, from Forbes: https://www.forbes.com/sites/chuckcohn/2014/09/15/build-vs-buy-how-to-know-when-you-should-build-custom-software-over-canned-solutions/#fa06cb8c371e

Committee of Public Accounts. (2013). *The dismantled National Programme for IT in the NHS.* London: House of Commons, UK Parliament. Retrieved March 14, 2020, from https://publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/294/294.pdf

Conn, J. (2013, February 12). *Blog: The right and wrong decision*. Retrieved April 1, 2020, from Modern Healthcare: https://www.modernhealthcare.com/article/20130212/BLOGS02/302129891/blog-the-right-and-wrong-decision#ixzz2VH4odsA0?trk=tynt

Department of Homeland Security. (2011). *REPORT ON THE ASSESSMENT OF THE SECURE BORDER INITIATIVE-NETWORK (SBInet) PROGRAM.* Retrieved April 8, 2020, from https://www.globalsecurity.org/security/library/report/2011/sbi-net-assessment.pdf

Doig, C. (2015, November 6). *How to determine when to build or buy enterprise software*. Retrieved April 21, 2020, from CIO: https://www.cio.com/article/3001357/how-to-determine-when-to-build-or-buy-enterprise-software.html

Fields, R. (1995, May 22). Build versus buy: Resist the seduction. *Chief Executive Magazine*(103). Retrieved April 22, 2020, from ProQuest: https://search-proquest-com.libproxy.ara.ac.nz/docview/212088346?OpenUrlRefId=info:xri/sid:primo&accountid=38794

Glick, B. (2014, February 5). *The BBC DMI project - what went wrong?* Retrieved April 14, 2020, from ComputerWeekly: https://www.computerweekly.com/news/2240213773/The-BBC-DMI-project-what-went-wrong

Government Accountability Office. (2010). *SECURE BORDER INITIATIVE DHS Needs to Strengthen Management and Oversight of Its Prime Contractor.* Washington, D.C. Retrieved April 8, 2020, from https://www.gao.gov/new.items/d116.pdf

Herrick, C. (2011, April 21). *Vic Police database project faces $100 million blowout*. Retrieved March 22, 2020, from Computerworld: https://www.computerworld.com/article/3485553/vic-police-database-project-faces-100-million-blowout.html

Hsu, S. S. (2008, February 28). *'Virtual Fence' Along Border To Be Delayed*. Retrieved APril 9, 2020, from Washington Post: https://www.washingtonpost.com/wp-dyn/content/article/2008/02/27/AR2008022703747.html

Kent, P. (2006, June 23). Don't develop software, buy it; better yet, get it free. *Boulder County Business Report, 25*. Retrieved April 22, 2020, from https://search-proquest-com.libproxy.ara.ac.nz/docview/221307401?rfr\_id=info%3Axri%2Fsid%3Aprimo

Kuranda, S. (2013, October 7). *Deloitte State Contracts Repeatedly Over Time, Budget: Report*. Retrieved March 26, 2020, from CRN: https://www.crn.com/news/channel-programs/240162344/deloitte-state-contracts-repeatedly-over-time-budget-report.htm?itc=refresh

Legislative Analyst's Office. (2012). *Employment Development Department's (EDD) Automation Projects.* Retrieved March 27, 2020, from https://lao.ca.gov/handouts/socservices/2012/EDD\_Automation\_5\_23\_12.pdf

Lister, S. (2004, August 9). *How £6bn computer system will help heal the NHS*. Retrieved March 14, 2020, from The Times: https://www.thetimes.co.uk/edition/news/how-pound6bn-computer-system-will-help-heal-the-nhs-26g208plkxb

Maughan, A. (2010, September 13). *Six reasons why the NHS National Programme for It failed*. Retrieved March 17, 2020, from ComputerWeekly: https://www.computerweekly.com/opinion/Six-reasons-why-the-NHS-National-Programme-for-IT-failed

Mazmanian, A. (2019, May 3). *Can anyone lead the $20B DOD-VA health IT modernization project?* Retrieved March 28, 2020, from FCW: https://fcw.com/articles/2019/05/03/ehr-dod-va-governance.aspx

National Audit Office. (2011). *The failure of the FiReControl project .* Department for Communities and Local Government, London. Retrieved April 6, 2020, from https://www.nao.org.uk/wp-content/uploads/2011/07/10121272.pdf

National Audit Office. (2014). *British Broadcasting Corporation Digital Media Initiative.* Retrieved April 14, 2020, from https://www.nao.org.uk/wp-content/uploads/2015/01/BBC-Digital-Media-Initiative.pdf

Office of Inspector General. (2011). *Homeland Security Grant Program Funds Awarded for Project Shields.* Department of Homeland Security, Washington DC. Retrieved April 3, 2020, from https://www.oig.dhs.gov/assets/Mgmt/OIG\_12-19\_Dec11.pdf

Panangala, S. V., & Jansen, D. (2013). *Departments of Defense and Veterans Affairs: Status of the Integrated Electronic Health Record (iEHR).* Retrieved March 28, 2020, from https://fas.org/sgp/crs/misc/R42970.pdf

PwC. (2013). *BBC Digital Media Initiative Review of the BBC’s management of DMI.* Retrieved April 14, 2020, from http://downloads.bbc.co.uk/bbctrust/assets/files/pdf/review\_report\_research/vfm/dmi/pwc\_dmi.pdf

Sampson, G. (2012). Whistleblowing for health. *JBPC*. Retrieved March 17, 2020, from https://www.grsampson.net/AWfh.pdf

Senate Committee on Post Audit and Oversight. (2014). *Massachusetts Information Technology Projects: looking Back, but Moving Forward.* Retrieved March 26, 2020, from https://malegislature.gov/Bills/188/S2107.pdf

Sessions, R. (2008). *Simple Architectures for Complex Enterprises.* Microsoft Press. Retrieved March 16, 2020

Standing Senate Committee on National Finance. (2018). *The Phoenix Pay problem: Working toward a solution.* Ottawa. Retrieved March 23, 2020, from https://sencanada.ca/content/sen/committee/421/NFFN/reports/NFFN\_Phoenix\_Report\_32\_WEB\_e.pdf

State Services Authority. (2011). *Inquiry into the command, management and functions of the senior structure of Victoria Police.* Retrieved March 19, 2020, from https://www.parliament.vic.gov.au/file\_uploads/InquiryCommandManagementFunctionsVicPolice2012\_DNVV27vr.pdf

Syal, R. (2013, September Wednesday). *The Guardian*. Retrieved March 17, 2020, from https://www.theguardian.com/society/2013/sep/18/nhs-records-system-10bn: https://www.theguardian.com/society/2013/sep/18/nhs-records-system-10bn

Ulfelder, S. (2003, June 2). *Buy! No, build!* Retrieved April 22, 2020, from ProQuest: https://search-proquest-com.libproxy.ara.ac.nz/docview/216085476/316F62ADB7484256PQ/1?accountid=38794

*Why SBINet has failed*. (2010, May 19). Retrieved April 9, 2020, from Homeland Security News Wire: http://www.homelandsecuritynewswire.com/why-sbinet-has-failed

Woolhouse, M., & Healy, B. (2013, October 4). *$54m later, state fired computer contractor*. Retrieved March 26, 2020, from The Boston Globe: https://www.bostonglobe.com/business/2013/10/03/thousand-defects-dor-fired-deloitte-august/vVptQAuFrhmDmGoqA2aI3L/story.html

Yurevich, D. (2019, October 7). *Build vs Buy: The Pros and Cons*. Retrieved April 21, 2020, from Syberry: https://www.syberry.com/company/blog/articles/build-vs-buy