13th European Conference on Research Methodology for Business and Management Studies, London, UK, 16-17 June 2014
http://toc.proceedings.com/22416webtoc.pdf

Critical Success Factors For IT Project Management: A Case Study Of A UK MOD IT Project

Annie Maddison Warren, Cranfield University, Shrivenham, Wiltshire, SN6 8LA, UK.
a.maddisonwarren@cranfield.ac.uk

Abstract: This paper examines Critical Success Factors (CSFs), tackling the lack of empirical research on public sector IT project management, using content analysis and considering the importance of context in case study research. Major government IT projects often end in costly failure, raising questions about whether CSFs are understood, applied and, if so, whether they have any impact. This study identifies twelve relevant CSFs, before examining their use through a case study of a major Ministry of Defence (MOD) IT project. The study of context reveals two overarching issues for government: the need for increased governance and to learn lessons. MOD Reports translate government policy to the Defence context, but there is little evidence of any impact on project initiation.

The case study suggests the benefits of spending more time on project initiation, expending resource on preparation rather than rushing into development, potentially a cultural problem within MOD procurement. There was an apparent lack of top-level engagement with this project initially, in terms of recognising it as strategic and allocating the necessary resources. The need to build relationships, communication and trust between contractor and supplier is overridden by the commercial realities of a contractual situation along with the apparent lack of awareness of the need to manage the contract beyond the delivery of requirements and the lack of competence to undertake that management.

The overarching conclusion is that the impact of CSFs is variable: ignoring them will have an adverse effect on performance, whilst applying them will strengthen the resilience of the project management but cannot guarantee success. This draws into dispute the use of CSFs as a project management tool, particularly with regard to the emphasis on 'success'. Although increased governance and control from central government appears to be a solution to IT project failure, it potentially forces generic

Copyright © The Authors. Published by Currans Associates. This is the Author Accepted Manuscript. Please refer to any applicable publisher terms of use.

solutions on to unique problems, further constraining action and potentially resulting in less reliable reporting in order to protect funding and resources. Generic CSFs are not the solution to the problems of major government IT projects, unique projects operating in highly specific and complex contexts; more contingent solutions should be sought. There needs to be greater recognition of this complexity, which makes these projects unpredictable, and more tolerance of error to allow learning.

Keywords: IT Project Management; Critical Success Factors; Public Sector; Content Analysis; Case Study

1. Introduction

In 2000, around 85% of UK public sector IT projects were in difficulty (Symonds 2004); a decade later, the cost of failing projects was estimated at around £26.3 billion, suggesting a lack of progress in tackling this problem (Savage 2010). However, there have been a series of investigations and reports on major government IT projects over the years to identify the Critical Success Factors (CSFs), defined as:

> …those few things that must go well to ensure success for a manager or an organization (*sic.*)...those managerial or enterprise areas that must be given *special* and *continual* attention to bring about high performance (emphasis in the original) (Boynton and Zmud 1984, p.17).

Outlined by Daniel (1961) and further refined by Rockart (1979), there has been a major academic research to identify CSFs. The resulting advice, guidance, methodologies, standards and training should have improved performance of IT project management in the UK public sector. However, continued and costly failure raises questions about whether project teams understand these CSFs, apply them and, if so, whether they have any effect. These questions are examined through a study of the UK Ministry of Defence's (MOD) Defence Information Infrastructure programme. DII is providing the infrastructure (hardware, software, data and network components) for Defence, connecting around 300,000 user accounts and 150,000 computers (DII IPT 2004). The discussion begins by exploring the organisation and structure of government in order to understand the context of this project before using undertaking a case study to gauge the extent to which CSFs have been understood and applied, and to what effect, before the implications of these findings are considered

and conclusions drawn about the validity of CSFs as a potential solution to IT failure in government.

2. Background

Used interchangeably for these purposes, the terms ‘public sector’ and ‘government’ are used to describe national, regional and local state organisations providing goods and services for citizens. ‘Project’ encompasses projects, ‘programmes’, meaning a number of interrelated projects, and ‘mega-projects’, describing their size, complexity and expense. More than a third of public sector IT projects in the UK have budgets greater than £1 million and, of these, four percent fit into the category of mega-projects with budgets greater than £50 million (Altshuler and Luberoff 2003). This reflects the complexity of government, which has 20 departments, over 200 agencies and 400 local authorities, arranged vertically with an insular culture (Butler Group 2004). Each has its own authority along with laws, codes and policies (Williams 1999). The tendency to operate on a national, rather than a regional, scale brings additional complexity. For example, driving licenses are administered centrally, not locally, as happens in other countries (Cross 2005). The resulting IT projects are often large-scale, highly ambitious, using leading-edge technologies, bespoke solutions and complex software, lengthening the development phase and raising the levels of risk (Brown 2001).

Inevitably, politics has a significant impact, making public sector organisations different to those in the private sector (Crawford and Helm 2009). Government is accountable to parliament, taxpayers, communities and businesses, working within complex legislative frameworks, but the maximum five-year period of a parliament means that this accountability is short term. A change in government results in a change in political direction and appointments (Crawford and Helm 2009, p.76). Alongside this, the UK suffers from ‘political hyperactivism’, the continual amendment and modification of legislation and regulations (Dunleavy et al 2004). Such alterations cause problems for IT projects, often resulting in a system design that no longer fits the requirement, as demonstrated by the doomed IT project at the Child Support Agency in 2003 (House of Commons, Work and Pensions Committee 2004).

The organisational structure results in decentralised IT projects and, thus, a proliferation of disparate, incompatible information systems, reinforcing the barriers between the departmental sub-cultures (Hackney and McBride 1995). Over the years, there has been little improvement in project management. The National Audit Office (NAO) (2009a), the body that oversees government in the UK, highlights the lack of priority given to learning the lessons of project failure despite the recognised benefits of learning from past experience. Dvir et al (2006) argue that identifying the relevant CSFs from past projects and using them to organise work activity on a new project improves success rates (Dvir et al 2006). To this end, the so-called McCartney Report, *Successful IT: Modernising Government in Action*, was initiated in 1999 to identify past lessons and inform future projects, whatever their context, so preventing the repetition of mistakes (Cabinet Office 1999).

The Report focuses on 10 areas that require attention in order to deliver successful results:

- Change management;
- Leadership and responsibility;
- Project management;
- Risk management;
- Modular and incremental development;
- Benefit realisation;
- Procurement and supplier relationships;
- Cross-cutting initiatives;
- People and skills; and
- Learning lessons.

Thirty recommendations included initiatives such as the Gateway Review Process, a system of sequenced appraisals to ensure that IT projects are viable, and the appointment of a Senior Responsible Owner (SRO) for each major project to ensure the delivery of projected benefits.

The McCartney Report was authoritative, based on sound work by experienced IT professionals. However, it is questionable whether its recommendations were fully

implemented or its lessons learned. McCartney himself notes a government failure to translate lessons into positive action (Cabinet Office 1999). However, declaring that "the process of implementing the recommendations cannot be allowed to stagnate", he allocated a delivery deadline, an SRO for each of his recommendations and a reporting process (Cabinet Office 1999, p.7). Despite this, progress reports ceased after two years as responsibility for implementation moved from the Cabinet Office to the Office of Government Commerce (OGC) in 2001 (Mugan 2005). An independent office of the Treasury, the now defunct OGC was established in April 2000 to improve central government procurement processes, make e-government a reality and manage individual IT projects. In line with the NAO, the OGC also noted a general failure throughout government to understand and consistently apply its lessons (Cabinet Office, Office of Government Commerce 2009a). The extent to which this is true is tested here through a case study of the DII Programme. The project team began work in the shadow of McCartney and should have been further enlightened by the series of reports that followed in its wake and reiterated its findings. Their management processes should, therefore, have been informed and influenced by the identified CSFs.

3. Research Methodology

The research began by identifying the CSFs. Content analysis of relevant reports led to a more precise, detailed and meaningful list of 12 CSFs. This was tested against CSFs identified in the general project management literature and the more specific IT project management literature then reviewed. This process confirmed the authenticity and accuracy of the CSFs, shown at Table 1, along with definitions highlighting the required activity, behaviour and skills, as well as the underlying issues.

The second stage was to assess the understanding and application of these CSFs, and whether they have improved performance. The selected methodology was case study, incorporating a number of methods, including interviews and surveys, and based on an interpretive research philosophy. The MOD began procuring DII in April 2003, awarding the contract to the Atlas Consortium, consisting of five companies, in March 2005. Interviews were held with 17 respondents, representing both the supplier and the project team, over a period of four years.

Table 1. CSFs for Major Government IT Projects

Affordability
An assessment of whether proposals can be paid for in terms of resources, cash flows and funding
Alternatives Certainty
Consideration of alternative approaches capable of fulfilling the objectives creates project confidence and commitment with the key stakeholders i.e. Do Nothing, Do minimum, Defer, Outsource, Consolidate
Benefits Certainty
Clear identification and definition of the business need for the project and the required performance improvement outcomes along with how these will be managed in terms of measures, owners, targets and strategic alignment
Change Readiness
The current state of the organisations involved in the project and their perceived ability to absorb, adapt to, and assimilate change
Clarity and Perception
Clarity of the rationale, scope and scale of the project and shared understanding by key stakeholders across broad communities involved
Competence and Capacity
The requirement for individuals associated with the project to be able to properly perform specific jobs through a combination of knowledge, skills and behaviour, along with the capacity, in terms of the availability of the right people with the right skills, to execute and effectively deliver the option
Complexity Management
The level of likely risk and the scale, novelty, diversity, interdependency and volatility of a project
Consistency and Coherence
Integration of the selected option with established systems, processes and policies
Constraints Certainty
An estimate of costs, resource requirements and timescales along with project planning, design and implementation
Scalability and Flexibility
Consideration of the versatility of a future option and its anticipated survivability in a future and unpredictable environment, requiring an understanding of the scalability (both up and down) and of the degree of flexibility
Stakeholder Management
The systematic identification, analysis and planning of actions to communicate with, negotiate with and influence all those who have an interest or role in the project or those who are impacted by the project
Value for Money
The project offers the optimum economy, effectiveness and efficiency in delivering the product along with a qualitative and quantitative judgement over the manner in which resources are utilised and managed and any reputational risk that has ensued to both public sector and supplier

Source: Author

4. The DII Programme: a Case Study

The UK government context has departments operating behind barriers with little overarching governance and IT projects based on over-optimism and underestimated

complexity, costs and risks. Internal MOD reports as well as reports by other bodies show that its poor record of project delivery, reflecting practice in the wider government context. This is compounded by the failure of project teams to control time, cost or to deliver value for money. In addition, the MOD has too many projects at any one time relying on insufficient funding, causing delays with new equipment, the continued maintenance of old equipment and rising costs (NAO 2009a).

The DII project team recognised the identified CSFs shown at Table 1 above. Some had read the McCartney report, others were equally aware of the reports that followed. Many also recognised the CSFs from departmental policy as well as from audits of the project. However, they do not face any repercussions if they are ignored, despite the stated government intent of improved project management practice and despite McCartney's decree that the implementation of his recommendations could not be allowed to stagnate. Despite this, the project team claimed to have understood and applied the CSFs. They examined similar projects in both the UK and the US to learn relevant lesson but stated that they had simply avoided repeating the same mistakes to the same degree, rather than avoiding them altogether. As the project matured, their experience became increasingly unique, presenting different problems and making the lessons learned from previous projects less relevant. Ultimately, there was no real comparator: the team developed their own specific solutions to their own distinctive problems, suggesting that learning external lessons has only limited utility in the early stages of a complex project.

Auditing bodies reported on this project positively. Although ambitious in scope, they thought the project well conceived, well organised, with sound governance, robust decision-making structures and continuity of key staff. The project team appeared to have understood and applied the CSFs with efforts to gain the necessary funding (Affordability); consideration of possible options to fulfil the requirement (Alternatives Certainty); clarity of the business need for the product (Benefits Certainty) and the need for organisational change (Change Readiness); shared understanding by key stakeholders (Clarity and Perception); the right people with the right skills (Competence and Capacity); tactics to manage risk (Complexity Management); a desired integration of established systems (Consistency and Coherence); awareness of cost, time and scope (Constraints Certainty); the adoption

of a modular and incremental approach (Scalability and Flexibility); recognition of the need to communicate with stakeholders (Stakeholder Management); and a requirement to run the project economically and efficiently (Value for Money). Despite this, the project was overspent and behind schedule. Given the MOD's approach to resources and risk, Affordability and Complexity Management were likely to prove problematic, imposing counter-cultural ways of working within this departmental context.

The team believed that they had managed Affordability. When the project was initiated, the department was close to lacking the funds to either maintain or to replace its current system, seeing no alternative to DII regardless of its financial basis. Although a key project, it was not given the required resources, based on a staged procurement with funding derived from discontinued legacy systems. The project was constantly seeking additional savings and its funding difficulties delayed some of the stages, meaning that legacy systems had to be maintained at cost. The need to initiate this project overrode special and continual attention to this CSF, Affordability, reflecting the attitude demonstrated by many previous MOD projects.

Complexity Management has also been problematic. Installation of hardware and software at numerous sites was based on a limited site survey, believing that the senior management imperative was delivery rather than preparation. The factory-style implementation, following the same process at each site, had been used successfully at another government department but one that had standard sites, uniform infrastructure and good quality communications. The MOD sites are very diverse with many in a poor state of repair, needing work to prepare for implementation. A full survey might have offset the expenditure and delay as the factory process went awry. However, the team clearly learned their lessons, working with the supplier to develop a more suitable implementation process.

The remaining 10 CSFs were recognised and appear to have been understood. However, their application was variable with differing effect. For example, Alternatives Certainty demonstrated 'group-think' with technical rationality dominating, rather than managerial or professional, which may explain the expectation failure on behalf of the users; there was inadequate Change Readiness in

terms of the preparatory work undertaken, with resulting cost overruns and delays; and Constraints Certainty showed inadequate through life costs and little regard for the financial and operational impact of delay. Giving CSFs 'special and continual attention' should 'bring about high performance'. Based on a review of the literature, performance was defined and measured as:

- Reducing the risk of escalation to cost, time and scope;
- Reducing the resource demands of cost, time and scope;
- Meeting the expectations of the stakeholders, including the project team, in terms of value and usefulness;
- Improving the scale or certainty of business benefits;
- Improving the scale or certainty of the project's contribution to defined strategic goals; and
- Avoidance of identified strategic environmental factors known to undermine delivery or future performance.

For DII, costs and timescales increased whilst resource remained largely static. Feedback from stakeholders has not been positive, although they recognise the requirement and some improvement in IT services. Business benefits are well tracked, although their scale and certainty has not been maintained. Risk was not avoided, threatening the project's contribution to defined strategic goals. In terms of environmental factors, the project has been hampered by changes to the MOD security policy and the effects of the financial crisis. Overall, it is not as robust as it might have been in terms of its performance.

The team recognised the CSFs, appeared to understand them and claimed to have applied them. Why did this not improve their performance? The above discussion shows that the context affected the attitudes and behaviours of the project team. They interpreted and applied the CSFs according to their culture and ways of working. The organisational bureaucracy and social norms of the MOD shaped their perceptions of these CSFs and the way they managed them. The project team can be charged with the well-recognised over-optimism, particularly in terms of funding, short cuts during

initiation, underestimation of risk, failure to control time, costs and to deliver value for money.

More generally, it appears that the government context is an obstacle to the imposition of standardised solutions. This suggests that context is highly significant, causing project teams to distort their management of the CSFs, replicating previously displayed norms, attitudes and behaviours. Therefore, lessons have to be applied with care and cannot be easily transferred between contexts.

5. Discussion

The DII project team acknowledged CSFs but managed its projects and procurement according its context. This confirms that organisations have difficulty in learning from past experience with dysfunctional patterns of behaviour allowed to continue, persistent reliance on the same processes with disregard for their failure to deliver (Robey and Newmand 1996). This may be due to the lack of central mandatory control in government, despite its apparently bureaucratic structure, with no penalties imposed if the CSFs are ignored, disregarded or if the very problems that McCartney highlighted are repeated. The only central constraints on IT projects in government departments are the Cabinet Office, which creates strategy, and the Treasury, which provides guidance on procurement (Anon 2010). However, neither has the over-arching authority or power to direct the actions of other departments (Mugan 2001). They cannot intervene with IT projects but can only persuade and attempt to build a common sense of purpose (Anon 2010). McCartney could only recommend, rather than demand compliance.

The NAO highlights the lack of priority given to learning in government departments, whilst high staff turnover leads to a loss of knowledge (National Audit Office 2009a). It has also recommended a central, mandatory system of assurance (National Audit Office 2010). Whilst recognising the positive impacts of some of McCartney's recommendations, such as the Gateway Reviews, the lack of an integrated system of oversight limits further improvements. The NAO (2009a) suggests a new assurance system to trigger necessary interventions, providing the ability to plan and resource

assurance activity, to systematically propagate lessons learned and so minimise the burden placed on projects.

In the US, the IT Management Reform Act (ITMRA), the so-called Clinger-Cohen Act, was introduced in 1996. It is designed to reduce IT project failure by forcing adherence to best practice and recognises the lack of accountability along with the culture of secrecy and cover-up (Collins 2004). All government agencies must have a Chief Information Officer (CIO), reporting to Congress if their IT project deviates from contract or price. This was enacted four years before McCartney declared that the UK Government "will not tolerate failure" (Simons 2000). However, the UK did not adopt similar legislative action, which may be fortuitous. Many consider the Clinger-Cohen Act a failure. CIOs are criticised for lacking appropriate skills and experience, having an average tenure of only two years, no budgetary authority and not reporting to their head of agency (Holmes 2010). In addition, government IT managers "routinely do not follow even some of the more basic project management practices" (Holmes 2010).

This suggests that governance and standardisation is not the answer to project failure in government. With influence based on informal relationships rather than authority, the focus should be on ensuring that departments are capable of operating in a complex, shifting environment with greater central authority to intervene on a highly selective basis when projects go awry. This discussion suggests that the lack of governance is due to the context of government, its federated nature and the fact that its different parts make their own decisions. Government appears to be a centralised organisation, meaning directive leadership and a specific decision making authority. In reality, it is decentralised, disparate and complex, with no clear leader, hierarchy or headquarters. In such a context, it is questionable whether CSFs can provide the means of tackling failure. Major public sector IT projects occur in a highly specific context that impacts upon them in potentially detrimental ways, whilst the lack of governance allows project teams to reject specified ways of working.

The complexity of these projects brings unpredictable risk from numerous sources (Cabinet Office, Office of Government Commerce 2009b). This needs to be recognised with greater tolerance of error to allow learning to take place openly. An

IT project might stray from its original objectives for many reasons but any changes, even if formally approved are likely to result in the charge of failure (Cabinet Office, Office of Government Commerce 2009b). It is questionable whether the same approach can be adopted across projects, whatever their funding, procurement, development or implementation model, with simply some fine tuning to reflect variety, scale and complexity. Attempts to improve procurement and management centrally may be rejected because they do not apply in unique contexts, requiring more variation. In other words, CSFs are context specific. Learning is more likely to come from experiences within the project. Rather than standardised solutions, projects teams need to learn from their own mistakes and apply their own solutions. This internal learning of lessons is more likely to lead to success.

6. Further Research

Despite the high profile failure of major government IT projects, very few sources specifically examine how they are affected by their context. Rosacker and Rosacker (2010) observe that the separate fields of project management, IT project management and public sector management are well developed, but that empirical research on public sector IT project management remains in its infancy. This single case study suggests that there needs to be further examination of the organisational culture and structure of government, the employee characteristics, the systems and, specifically, how they are deployed and how they impact on major IT projects. This would give a better understanding of the conditions in which these projects are developed and their effect on the potential value of those projects.

7. Conclusion

This study considers the impact of CSFs on a major government IT project. Technology is seen as a means of making government more effective and efficient. In these straitened times, it is imperative that these projects deliver successful outcomes. CSFs provide a means to do this. However, this study shows that their impact is variable: ignoring them will have an adverse effect on performance; applying them will strengthen the resilience of the project management but cannot guarantee success.

This draws into dispute the use of CSFs as a project management tool, particularly with regard to the emphasis on 'success'. The notion that managing 'a few key areas' will deliver success and that these are applicable to all projects in all contexts is too simple for an increasingly complex world with increasingly complex projects. Although increased governance and control from central government appears to be a solution to IT project failure, it potentially forces generic solutions on to unique problems. It is apparent that generic CSFs are not the solution to the problems experienced with major government IT projects, unique projects operating in highly specific and complex contexts; more contingent solutions should be sought. There needs to be greater recognition of this complexity, which makes these projects unpredictable, and more tolerance of error in order to allow learning to take place.

References

Altshuler, A. and Luberoff, D. (2003) *Mega-Projects: The Changing Politics Of Urban Public Investment,* Brookings Institution, Washington, DC.

Anon. (2010) "A Stronger Hand", *GC: Government Computing Magazine,* April, p.22.

Boynton, A.C. and Zmud, R.W. (1984) "An Assessment Of Critical Success Factors", *Sloan Management Review,* Vol. 25, No. 4, pp 17-27.

Brown, T. (2001) "Modernisation Or Failure? IT Development Programmes In The UK Public Sector", *Financial Accounting and Management IT,* Vol. 17, No. 4, November, pp 363-381.

Butler Group (2003) "Improving Public Sector Projects", [online] Retrieved October 9, 2004, from www.butlergroup.com

Cabinet Office (1999) *Successful IT: Modernising Government In Action.* HMSO, London.

Cabinet Office, Office of Government Commerce (2009a) *Major Projects Review Group,* HMSO, London.

Cabinet Office, Office of Government Commerce (2009b) *Programmes And Project Delivery: Joint Statement Of Intent.* HMSO, London.

Collins, T. (2004) "Minister To Consider Computer Weekly's Plan To Stop IT Disasters", *Computer Weekly,* 6th July, p 14.

Collins, T. (2009) "What MPs Said About The State Of IT Projects In 1984", [online], C*omputerWeekly.com,* 12 November, Retrieved November 18, 2010, from http://www.computerweekly.com/blogs/public-sector/2009/11/public-accounts-mps-attack-it.html

Crawford, L.H. and Helm, J. (2009) “Government And Governance: The Value Of Project Management In The Public Sector”, *Project Management Journal*, Vol. 40, No. 1, pp 73-88.

Cross, M. (2005) “Special Report: Public Sector IT Failures”, *Prospect*, October, pp 48-52.

Daniel, D.R. (1961) “Management Information Crisis”, *Harvard Business Review*, Sept-Oct, pp 111-121.

DII IPT (2004) *Defence Information Infrastructure: One Information Infrastructure.* DII IPT, Copenacre.

Dunleavy, P., Margetts, H., Bastow, S. and Tinkler, J. (2004) “Government IT Performance And The Power Of The IT Industry: A Cross-National Study”, *Annual American Political Science Association Conference. Panel 25-2, Digital Policy Issues: Inequality, E-government*, [online], Retrieved February 15, 2013, from http://www.governmentontheweb.org/sites/governmentontheweb.org/files/Government-IT-Performance.pdf

Dvir, D., Ben David, A., Sadeh, A. and Shenhar, A.J. (2006) “Critical Managerial Factors Affecting Defense Projects Success: A Comparison Between Neural Network And Regression Analysis”, *Engineering Applications of Artificial Intelligence*, Vol. 19, No. 5, pp 535-543.

Hackney, R.A. and McBride, N.K. (1995) “The Efficacy Of Information Systems In The Public Sector: Issues Of Context And Culture”, *The International Journal of Public Sector Management*, Vol. 8, No. 6, pp 17-30.

Holmes, A. (2010) “Five Reasons Why Clinger-Cohen Failed”, *NextGov: Technology and the Business of Government*, [online], Retrieved November 26, 2010, from http://techinsider.nextgov.com/2010/08/five_reasons_why_clinger-cohen_failed.php

House of Commons, Work and Pensions Committee. (2004) *Management Of Information Technology Projects: Making IT Deliver For DWP Customers (*HC 311, Third Report, Session 2003-04). HMSO, London.

Kirkpatrick, D. (2009). “Lessons From The Report On MOD Major Projects”, *RUSI Defence Systems*, June, [online] Retrieved January 10, 2010, from http://www.rusi.org/downloads/assets/Acquisition_Issues_Lessons_from_the_MoD_RDS_Summer_09.pdf

Mugan, C. (2001) “Cabinet Office Loses Key IT Responsibility”, *ComputerWeekly.com*, [online], Retrieved March 30, 2005, from http://www.computerweekly.com/SiteMapArticle/Articles/2001/04/27/c5791/179830/CabinetOfficeloseskeyITresponsibility.htm

National Audit Office (2009a) *Helping Government Learn.* HMSO, London. [online], Retrieved January 20, 2011, from http://www.nao.org.uk/publications/press_notice_home/0809/0809129.aspx

National Audit Office. (2009b). *Major Projects Report 2009*, HC85-I. London: HMSO, [online], Retrieved January 14, 2011, from http://www.nao.org.uk/publications/0910/mod_major_projects_report_2009

National Audit Office (2010) *Assurance For High Risk Projects*, HMSO, London, [online], Retrieved January 20, 2011, from http://www.nao.org.uk/publications/1011/project_assurance.aspx

Public Accounts Committee (2009) *Defence Information Infrastructure*: *First Report Of Session 2008-09*, HC100. HMSO, London.

Robey, D. and Newmand, M. (1996) "Sequential Patterns In Information Systems Development: An Application Of A Social Process Model", *ACM Transactions on Information Systems*, Vol. 14, No. 10, pp 30-63.

Rockart, J.F. (1979) "Chief Executives Define Their Own Data Needs, *Harvard Business Review*, Mar-Apr, pp 81-93.

Rosacker, K.M. and Rosacker, R.E. (2010) "Information Technology Project Management Within Public Sector Organizations", *Journal of Enterprise Information Management*, Vol. 23, No. 5, pp 587-594.

Savage, M. (2010) "Labour's Computer Blunders Cost £26bn", *The Independent*, 19th January, [online], Retrieved March 29, 2010, from http://www.independent.co.uk/news/uk/politics/labours-computer-blunders-cost-16326bn-1871967.html

Simons, M. (2000) "Failure Is Not An Option In Government's Review Of IT", *www.computerweekly.com*. May, [online], Retrieved February 21, 2013, from http://www.computerweekly.com/feature/Failure-is-not-an-option-in-Governments-review-of-IT

SOCITM (2010) "SOCITM's Response To The Spending Review", *SOCITM's Webpage*. 21 October., [online], Retrieved December 2nd, 2010, from http://www.socitm.net/press/article/152/socitms_response_to_the_spending_review

Symonds, M. (2000) "Survey: Government And The Internet: The Next Revolution", *The Economist*. 22nd June, [online], Retrieved October 9, 2004, from www.economist.com/surveys/showsurvey.cfm?issue=20000624

Williams, N. (1999) "Modernising Government: Policy Making Within Whitehall", *The Political Quarterly*, Vol. 70, No. 4, pp 452-459.



https://dspace.org/

Critical success factors for IT project management: a case study of a UK MOD IT project

Warren, Annie Maddison

2014-06-30
Academic Conferences Ltd
http://connection.ebscohost.com/c/case-studies/96270526/critical-success-factors-project-management-case-study-uk-mod-project
Maddison Warren A (2014) Critical success factors for IT project management: a case study of a UK MoD IT project. In: 13th European conference on research methodology for business and management studies (ECRM 2014), 16-17 June 2014, London, UK

Downloaded from a DSpace repository. https://dspace.org/