## This paper is a draft chapter from

## our book, that should instead be cited:

**Gauld, R and Goldfinch, S with Dale, T**

**Dangerous Enthusiasms: E-Government, Computer Failure and Information System Development**

**Otago University Press 2006**

# Pessimism as an Information System Management Tool in the Public Sector: Lessons from the INCIS Fiasco in the New Zealand Police Force

**Tony Dale**

**Department of Computer Science, University of Canterbury**

**Private Bag 4800, Christchurch, New Zealand**

**e-mail: Tony.Dale@canterbury.ac.nz**

**Shaun Goldfinch**

**Department of Political Science, University of Canterbury**

**e-mail: shaun.goldfinch@ canterbury.ac.nz**

.

**Pessimism as an IS Management Tool in the Public Sector: Lessons from the INCIS Fiasco in the New Zealand Police Force**

The majority of information system (IS) developments are unsuccessful.[1] The bigger the development, the more likely it will be unsuccessful. While exact numbers are uncertain, and depend to some extent on how success is measured, something like 20 to 25 percent of all projects are total failures, while 30-60 percent are partial failures. The minority are those counted as successes (Collins and Bicknell 1997; Heeks and Bhatnagar 1999; Heeks 2002; Iacovou 1999; James 1997; Korac-Boisvert and Kouzmin 1995). In a US survey of IS projects by the Standish Group, for example, it was found that success rates varied from 59 percent in the retail sector, to 32 percent in the financial sector, to 27 percent in manufacturing, and 18 percent in government. Overall, the success rate was 26 percent. Forty-six percent of projects had problems including being over budget and behind schedule, or being delivered with fewer functions and features than originally specified. Twenty-eight percent failed altogether or were cancelled. Cost overruns averaged nearly 200 percent. This success rate varied dramatically by total project budget: at less than US$750 000 the success rate was 55 percent; with budgets over $10 million, *no* projects were successful (SIMPL/NZIER 2000). Another survey found that between 30 and 40 percent of all IS projects exhibited some degree of escalation (Keil, Mann, and Rai 2000).

The sums involved can be mind-boggling. A study of IS developments (ISD) in the British public sector estimated that 20 percent of expenditure was wasted, while a further 30-40 percent led to no perceivable benefits (Wilcocks 1994). In 1994 the

US General Accounting Office reported that the spending of over $200 Billion in the previous 12 years had led to few meaningful returns. Collins and Bicknell (1997) estimated public sector failures in the UK have cost 5 billion pounds. For example, the UK's public health service Resource Management Initiative led to new Information Systems introduced into almost every hospital. Despite the expenditure of hundreds of millions of pounds, few were successful 'by any criteria' (Heeks and Bhatnagar 1999, 59). The Wessex Health authority's Regional Information Systems Plan was cancelled after something between 43-60 million pounds (the actual figure was uncertain) had already been spent, with almost nothing achieved (Collins and Bicknell 1997). A benefit payment scheme involving the British Post Office, the Department of Social Security and the computer company ICL, was abandoned after three years at the cost of 300 million pounds (Economist 2002). An already obsolete air-traffic support system opened in Swanson, UK, in 2002, six years late and 180 million pounds over budget (Economist 2002). Vast sums of money, mostly provided by aid agencies, have been spent on health information systems in South Africa, on donor funded IS projects in China and on World Bank funded projects in Africa – all of which have been total or partial failures (Heeks 2002). Spectacularly, the US Internal Revenue Service, with an annual computer budget of $8 Billion, has managed 'a string of project failures that have cost taxpayers $50 billion a year [mainly defined as revenue forgone] – roughly as much as the yearly net profit of the entire computer industry' (James 1997, 1).

New Zealand has not been immune to IS failures. Recent public sector failures included a Health Waikato project which was abandoned at the cost of NZ$9 million, the failure of a large part of a NZ$26 million project by Capital Cost Health,

and the Landline project which was late and NZ$52 million over budget (Espiner 2000). In a report to the New Zealand Department of the Prime Minister and Cabinet, it was found that 38 percent of all private and public sector projects were judged a success, 59 percent were found to have involved problems and 3 percent were judged a complete failure or were cancelled. Government success rates, at 38 percent, were slightly higher than private sector success rates, at 31 percent (SIMPL/NZIER 2000). At less than NZ$500 000 the success rate was 80 percent for the government and 41 percent for the private sector, while at $2-10 million the failure rate was 20 (public) and 22 (private) percent. At the over NZ$10 million mark, the success rate for both was zero.

Drawing on published accounts, archival material obtained through the *Official Information Act* 1982 and interviews with contractors and government officials, we examine and draw lessons from the largest public sector IS failure in New Zealand's history – the collapse of the Police Integrated National Crime Investigation System (INCIS). INCIS was a highly ambitious development, to be based around yet-undeveloped technology, with 3125 personal computers linking all police stations to each other and to a national crime database. It was promoted as improving criminal investigation and analysis for the police and as increasing their administrative and operational functions, all without increasing the demands on the police and government budget. It would, it was claimed, save on paperwork, freeing up police for front line duties and leading to job savings. However, after several years of cost and timetable overruns, management problems, and the non-delivery of applications, the project was abandoned in 1999 at the cost to the government, after an out-of-court settlement with IBM and sale of the project equipment, of around

NZ$100 million. This was for something that finally delivered little more than e-mail. The Police were left with an organisation 'reengineered' around a 'Community Policing Strategy', which was to be based around a functional INCIS system. The loss of $100 million, mostly out of an annual Police budget of around $800 million,[2] put severe pressure on Police budgets. Although problems with INCIS were increasingly reported in the media over the life of the project, Government monitoring regimes were ineffective in controlling the project. The INCIS fiasco encouraged a report by a select committee of the New Zealand parliament and a Ministerial inquiry, and a review of IT monitoring regimes in the public sector. It was not until a change of government that the project was admitted to be a failure.

While having some unique characteristics, the INCIS fiasco showed many of the traits of the typical failed IS project. These included highly overblown expectations regarding IS; the attempted development of new and unproven technology; management and reporting problems; a naive faith in contracts to control development and seek redress when things went wrong; and increasing the complexity of the project through specification changes and organisational restructuring. While there is a large body of literature on IS failures proposing a variety of solutions to the problem, we argue that these searches for 'silver bullets' or 'techniques', whether the latest management fad or new programming technology, largely miss the point and are possibly doomed to failure. Instead, we propose an approach to IS development in the public sector that is often lacking in projects: that of pessimism. This is the belief that in general the processes of software and IS development are so complex, so full of uncertainty, so ridden with human error, the clash of personalities and interests, the dysfunctions found in organisations and so on, that large projects will generally fail.

These problems are inherent in the development of these large and complex projects, and cannot be simply fixed by new and better technology, by superior management structures or the appointment of hero-managers. Pessimism is an explicit rejection of the naive faith and optimism placed in technological and management fixes, and the promises of IS salesman and consultants. Instead it argues that large, optimistic and ambitious IS change should be avoided in the public sector. It recommends a public manager as a curmudgeonly, risk-adverse, sceptical and suspicious adopter of technology – virtually the opposite of the business-like entrepreneurial manager of new public management ideology – standing back from the whirl of the flash and new, and instead supporting the proven, the modest, the uninspiring, the possibly grey promises of smaller adaptation of technology, of incremental change to management processes - if indeed adopting new technology is desirable at all.

**The INCIS Project**

In the 12 years before INCIS at least six major Police IT systems had been implemented, most of which had failed to progress for a variety of reasons, including a lack of support from the organization (Sapphire 1994). This did not discourage further projects however, and Police were keen to move away from the mainframe-based system known as the 'Wanganui computer'. This was essentially a powerful record keeping system that first went into operation in December 1976 and had grown incrementally since through various upgrades.

The origins of INCIS go back as far as 1985 when Project Serious Incident Computer Applications began in April. In November 1990, Azimuth Consulting

reported on a number of IS requirements for Police Systems, which include INCIS. This was further developed by Police. A Price Waterhouse Report of 13 November 1991 made a number of suggestions on the concept of INCIS and they were then contracted to further develop the project. In December 1991 a scoping study was delivered. A proposal was presented to what was called the National System Steering Committee on 10 September 1992, and the Police Executive Committee authorised the project team to issue as a request for information (RFI), a request for tender (RFT) and to prepare a business plan to present to Cabinet (Small 2000, 35). The RFI was issued in November 1992 and sent to 141 potential suppliers, with 69 responses received. Of these, four were selected and sent a RFT, requesting a fixed price contract. Tenders were received from Andersen Consulting and IBM, with an evaluation favouring IBM. Both were asked to rebid, and these were analysed on the INCIS Project Tender Rebid Evaluation of 12 July 1993, which was again favourable to the IBM tender. The INCIS business case was prepared by Police by May 12th, 1993, with Tony Crewdson, the future project director, instrumental in its development. This was extremely ambitious, outlining a series of functions that were not in existence elsewhere. That police ambitions were great was confirmed by Police visits overseas in 1993 which could not find similar systems in operation and Tony Crewdson, the INICS project manager noted that no one else had yet developed a system that 'met the needs' of police (Jackson 1998). This should have immediately rung alarm bells that these 'needs' may have been somewhat ambitious.

INCIS was to be a highly ambitious project, combining all police databases and linking them to all stations through a network of 3125 PCs. Police would be to enter their notes directly onto PCs and be directly interfaced with other aspects of the

Justice system. Proposed 'speedbooks' would allow relevant files to updated automatically as data was entered. It was claimed that INCIS would deliver benefits of $NZ5337.7 million over its lifetime. This included the freeing up 1.9 million hours of police time annually, at a benefit of $72.3 million. This was to be delivered through reduced paperwork, a flatter hierarchy and improved work-flows. It would also save around $14.2 million on the systems then being used – the LES and NIS (the Wanganui computer). Funds would also be generated by allowing other departments to use INICS on a 'user pays' basis, and by expected overseas sales revenues of $45 million over the life of the project. It also promised a number of other benefits such as increased officer safety, improved crime prevention and detection and an improved relationship with the community. These promised benefits were extremely optimistic, to say the least, if not verging on the fantastic. Some feeling for the huge complexity of INCIS can be given by the large numbers of staff engaged in its development: by the time of its termination, 25 IBM employees, 125 contractors and an 'unspecified number of police staff' were involved in the project (Beynen 1999, 1).

The police consulted with various government departments, including the central agencies and Ministry of Justice who 'believed that an integrated approach to the development of IT systems in the area of criminal justice if maximum efficiency benefits were to be obtained' (Waitai 1999). A review by Ernst and Young, dated 22 July 1993, commissioned jointly by the Treasury and Police to report on 'strategic considerations', the Business Case and the preferred IBM bid, concluded that the INCIS case was 'based on a sound technical solution', was ' consistent with the corporate strategy of Police,' and that it had 'a well argued business case for an affirmative investment decision' (Ernst & Young 1993, 4). However the report raised

a number of reservations, including the level of overseas development involved, the need for 'proof of technical viability and deliverability', and the need for the implementation plan to be competed before the completion of the contract negotiations (Ernst & Young 1993, 8).[3] The Minister of IT, Maurice Williamson, also noted a number of concerns with the "INSYS" (sic) project in a meeting with the Police Commissioner, including the long-time viability of the planned OS/2 operating system and the possible costs and delays of converting this to Windows NT, 'the grandiose' nature of the project and problems with training and support (Williamson 1993).[4] A Request for Proposal was issued to IBM on 3 December 1993. On 31 January 1994, KPMG recommended continuing with OS/2 and reported that the INCIS project was consistent with the Police Information Technology Strategy (Small 2000, 40).

After various papers were presented to March and April in 1994, Cabinet approved the proposal, which had changed somewhat from the original business plan.[5] The cost was now estimated to be $203.64 million, with capital expenditure comprising $98.7 million and operating expenditure comprising $105.81 million. This was to be spread over the lifetime of the project of eight years including the expected two and a half years of development. The Government was to contribute $62 million in capital contributions, while the Police would fund the rest within its existing budget. The efficiency gains, mainly to be delivered by saving of around 11 percent of the hours worked by policy personnel, were expected to deliver $380 million, with 30 percent to be delivered to the Crown.[6] These savings were mainly to be delivered by reducing sworn personnel by 540 by June 2000 (Waitai 1999). Even within the government, Police projections on INCIS were treated with some

scepticism (Fisk 1993). KPMG advised again that the Police should continue with OS/2. On 31 August Price Waterhouse withdrew from the project, and the Project Manager, Carr, now with Sapphire Technology Limited, prepared a handover report. This noted a number of problems and risks with INCIS (Sapphire 1994). These were seen to be manageable by the Project Sponsor.

*The INCIS project begins*

Following Cabinet approval, the Police completed negotiations with IBM and signed the contract in September 1994. The INCIS Request for Proposal (RFP)[7] and contract amounted to over 4,000 pages, the largest IT contract in New Zealand's public sector history, and possibly the largest IT contract, public or private, in New Zealand's history. The Police then established an INCIS project team with Superintendent Tony Crewdson as Project Director. Crewdson had no experience in the management of large IT projects. To manage the organizational change and restructuring that was to accompanying INCIS, a Change Management Team was established, reporting directly to Deputy Commissioner of Resource Management (and later Commissioner) , Peter Doone. Doone was initially the INCIS project sponsor, appointed in June 1993. Price Waterhouse was appointed to audit the INICS project in December 1994.

The INCIS program was designed to be delivered in two sections. The first was to install PC networks in all Police stations replacing the Wanganui systems 'with new Suspect and Offence Information Systems, Crime Trend Analysis, Intelligence Analysis and Mail Facilities.' The second was to implement a 'Case and

Investigation System' early in 1997 (Small 2000, 28). This later changed to iterations one, two and three (with Release one) and then to Increment One, Two and Three.

The delivery of the first release of INCIS was scheduled for April 1995, with the second (with new INCIS applications) in July 1995. However, problems were evident from the first and projected completion dates slipped. The 'INCIS Liaison Update Newsletter' of January 1995 projected the first release as being completed by the end of 1996, and the second implemented in early 1997, but in January 1995 Cabinet papers proposed the first delivery in March 1997, the second for December. Costs were also blowing-out. The INCIS Project Status Report of June 1995 noted the 'effort and resources required to complete… will be considerably larger than originally anticipated (Crewdson 1995, 13). The October 1995 Price Waterhouse report reiterated noted that the slippage in delivery dates was of concern.

INCIS began with a supposedly complete specification in the Request for Proposal and contract. However, the Police and IBM project teams became aware during February/March 1995 that the Contract specifications were not detailed enough to begin the design of INCIS, and so between March and October 1995 operations "Discovery" 1 and 2 were carried out to create detailed specifications for the implementation of the INCIS applications.

Management problems soon became evident. The Sapphire report of August 31st, 1994 noted 'Police has been very slow in making decisions. This appears to be worsening, rather than improving.' In May 1995 partnering meetings between IBM

and the Police were abandoned and replaced by an Executive Control Group to try to reduce the dependence on IBM. This was supported by the Police director of IT (Batchelor) but opposed by the INCIS Project Director (Crewdson). Personality disputes between the two became particularly heated as Batchelor and Crewdson offered his resignation during 1995 (Waitai 1999). Bachelor even claimed that the report of December 1996 on the project was misleading (something denied by Doone (1999))[8], called into question Crewdson's competence, and saw Crewdson as having too close ties to IBM (Justice and Law Reform Committee 1999). For his part, Bachelor was instrumental in pushing for specification changes that increased the complexity of the project. The relationship was particularly complicated, as while Crewdson had been appointed 'Project Director' in October 1994, this was somewhat of a misnomer and he reported to Greg Batchelor, appointed as Director of IT in November 1994, something that he was not necessarily comfortable with (Justice and Law Reform Committee 1999).

Technology changes were also signalled within the first year of the project with police considering making changes to the wide area network, the local area network and the desk top operating systems. In May 1996, the Police requested that the 'client' operating system be changed from IBM's OS/2 to Microsoft Windows NT. The linking of Windows NT desktops to OS/2 server login was 'world first' development and Police were advised by IBM that an immediate move to Windows NT desktops and an OS/2 server was not feasible with the technology available at that time. This decision to switch from OS/2 was also not supported by Crewdson, the project director, but was by the I & T Director, Greg Bachelor and Maurice Williamson, the Minister of IT (Matthews 1996). In July 1996, IBM advised the

police that guarantees in regard to the performance and response time were to be waived because of the change to Windows NT and the network. The Police, however, pressed ahead and agreement was reached on 14 October 1997. IBM absorbed an additional $10 million for the cost of the changeover, while Police contributed $1.5 million. Police also pushed for a change from the Token Ring Local Area network to Ethernet, despite two evaluations supporting the Token ring. After negotiation, 'customer preference' was the reason imposed by Police for the changes. The Wide Area Network was also changed, avoiding the usual change process and without competitive tendering (Waitai 1999).

> In March 1996 Price Waterhouse reported:
>
> > At its half way point the project faces a number of serious issues that may prevent its completion on time and within budget. Project management note that there is little or no contingency remaining and we believe that there is legitimate reason for concern at this point that the delivery dates will not be met.
> >
> > The key issue facing the project at present is the selection of the appropriate system architecture for the INCIS project and the impact this decision has on the project deadlines and on the overall Police I&T strategy. At that date of this report the review is still to be finalised (Price Waterhouse 1996, 2).

Price Waterhouse described the INCIS project as high risk in a June report, but in later reports described INCIS as very high risk. However, Police reports continued to reassure the government that the project was achievable, despite the difficulties. In a December 1996 response to the Price Waterhouse report, Crewdson noted that Police and IBM Project management saw the project as high risk and noted that delays in the provision of information from IBM had heightened this perception of risk, but saw the

'potential cost exposure' as manageable with IBM 'willing to make substantial concessions'. Crewdson also noted that the establishment of a Project Steering Committee and that the recruitment of 'highly skilled' technicians and management would ensure adequate control (Crewdson 1996).[9]

By early 1997 monitoring agencies were aware the project was facing difficulties. In February the Treasury were already voicing concern regarding the reporting on INCIS, noting the non-production of the September 1996 INCIS report (Secretary to 1997a), while the State Services Commission noted 'whispers' about the state of the INCIS project, including that the project was 'at least 6 months behind schedule' and that the 'Police's current funding proposals [included] a request for reinstatement of $10 million a year which represents much of the promised INCIS savings'(Rapley 1997) . In March the Secretary for the Treasury wrote to the Treasurer and the Minister of Finance noting that INCIS was 'behind schedule by 9 months' and 'forecast to cost $104 million, rather than the original budget of $97 million' with the 'potential for additional cost overruns (Secretary for the Treasury 1997b).'

In response to such concerns, a joint review was commissioned by the Treasury and Police, to be conducted by Andersen Consulting. Andersen reported in May 1997 that around $55 million had been expended or incurred of the $95 million budget, with projected cost overruns of $8 million. It also reported that the project was eight to twelve months behind schedule. While Andersen noted there was 'considerable risk' associated with the project, it recommended it be continued and that Police better manage the project and contract. The Treasury were aware the situation was even

more serious than Andersen allowed, noting in June that the cost overruns of INCIS could be $20-50 million, and discussing the possibility of project termination (Treasury 1997).

In response to these problems, an Executive Control Group was established consisting of the Deputy Commissioner of Police, the Police Director of Information and Technology, the Police INCIS project director, the Managing Director of IBM (NZ), the Solutions Integration Manager (IBM Asia Pacific) and Project Manager (IBM NZ). The group was to meet fortnightly to monitor and review the project. In March 1997 the then director of Police IT, Greg Bachelor, resigned. In June 1997 the INCIS Project Internal Audit noted the continual 'deterioration in the relationship between IBM and Police', the 'lack of access to IBM personnel' and the inability or unwillingness of IBM to respond to questions in writing (Price Waterhouse Coopers 1997, 2).

In September 1997 a fundamental change was made to the software system architecture: the new and untried (and ultimately unsuccessful) software technology of distributed OO client/server was replaced with a conventional three-tier client/server architecture, with INCIS applications to run on IBM's proprietary CICS (applications environment) and MVS (mainframe operating system) platform.[10] The fundamental software architecture of INCIS was completely changed, which required substantial respecification and rewriting of the system. A magazine article by Chamberlain (1997, 43) noted INCIS 'was due to be operational in March this year [1997] but hitches (chiefly a switch from IBM OS2 to a Windows system) have put it

a year behind'. However, as a former contractor noted in an interview, the INCIS software implementation was at the time being completely restarted. A further systems analysis, Operation Obstat, was carried out from 18 September to 31 November 1997 to respecify what was required to complete the INCIS contract, and on Dec 5th, 1997, Police and IBM signed a deed of variation of contract. The variation involved the commitment of a further $20 million for more development work. According to interviews, IBM threatened to withdraw from the project unless this amount was forthcoming. This sum was contracted for by Police without the required authority from Cabinet, and a Cabinet minute of May 18th, 1998, directed a review of the contractual arrangements between Police and IBM. The Treasury only became aware of the contractual variation from the press. The Cabinet moved to accommodate the unauthorised expenditure, but directed that the Police Commissioner's delegated spending authority be reviewed (Waitai 1999). The ministers of Finance, Police and the Associate Treasurer of directed that an independent external review of Police administrative and management levels and structures be carried out 'in order to identify opportunities for achieving efficiency [financial] savings' (Minister of Police t al 1998).

In October 1997 rumours were circulating in the Police and outside the government that delays in the INCIS project were due to 'costly cockups' (Chamberlain 1997, 43). The IT project director Tony Crewdson, noted that the 'reality is we can't prove [the benefits] until the thing is up and running. We are not dazzled by technology. It's only a tool. Used wisely, tools can provide a lot of relief. However, Chamberlain reported that 'police of all ranks are sneeringly cynical at the

notion that being able to take a laptop in the squad car will compensate for fewer staff.'

From December 1997 to August 1998 IBM delivered more than 3,000 workstations and associated hardware to the Police. This represented a significant proportion of the value of the contract to IBM. However, almost no INCIS applications were available at this stage. The cost of infrastructure 'appeared to be the full retail price without any significant reduction for bulk or other factors. It is perceived that the pricing of hardware cross subsidised, to some degree, IBM software costs' (Small 2000, 152).

In May 1998 the Cabinet approved a further $1 million to strengthen the project management. An external expert was recruited as INCIS project manager in October 1998 and a KPMG Peat Marwick partner was appointed to the INCIS Executive Control Group. There was also pressure on Crewdson to resign with the SSC noting that 'the incumbent project director has been off-site since May and Police are negotiating with him about his future employment within, or outside of Police." (Provost 1998). Crewdson left the INCIS project in May 1998 and the Police in October 1998, to be replaced by Stewart Watson.

In the face of continual questions regarding INCIS, an Ad Hoc Official Committee for IT Monitoring was also established in May 1998 chaired by the Deputy State Services Commissioner. The Police were required to report monthly to the committee. In June 1998, Andersen Consulting presented a report examining to what extent the

Police had complied with the previous report of May 1997. As the Treasury noted, the revised contract ‘did not include end to end performance guarantees...’, while it was noted the Police did not explore options to the project, and the project timetable had ‘no allowance for delays nor was a specific amount of money set aside for cost overruns as is normally the case with large projects (Shennan 1999).’

To allay their concerns, the Treasurer Winston Peter and the Secretary to the Treasury visited senior IBM executives in New York. Assurances were given that the project would be completed, although no timeframe was given, and IBM made available additional staff to work on the project. A law firm, Philip Fox, was engaged by the Police and Treasury to undertake a review of the varied contract, in the wake of the extra unauthorised $20.17 million allocated. Police then notified other government officials in February 1999 that further delays were expected. The progress of increment 1 and 2 were reviewed, and it was found ‘that increment 1 was being managed in accordance with the best practice project management techniques’ (Waitai 1999) (!) Police also received a detailed project plan from IBM for increment 2. Bordering on the ludicrous, the "INCIS Increment Two Project Scope Review" stated in April that ‘Police appeared to have managed this project extremely well, to the point of calling it ‘perfect project management.’’ However termination of the project was already being considered with a Police letter to the SSC listing a number of implications for the cancellation of INCIS, including legal liability to IBM for up to the full value of the contract ($94M) less funds paid to date ($67M), and releasing IBM from liability for $30M in extra application development costs (Matthews 1998).

On Jan 11th, 1999 the Ad-Hoc Committee on IT claimed ‘mechanisms have been put in place to facilitate effective management of the identified risks’ and estimated the cost to complete the INCIS project at $119 million (Mathews 1999, 5-6). A report by the in early 1999 by the Gibraltar Groups estimated that the cost to complete INCIS would now be in the region of capital costs of $156 million and operating costs rising to $70 million in 2000/2001, with a likely extension of 12 months over its expected June 1999 completion (Soar 1999). The expected completion date moved out to May 2000 for increment 1 and November 2000 for increment 2, and the Treasury were aware that the slippages, which they blamed on IBM, were becoming out of control. While continuing the project was also canvassed, the abandonment of the project was also being openly considered (Treasury 1999). Because of the delays of INCIS, the LES police IT system also required alterations to enable it to run after the year 2000 (i.e.: to fix the ‘Y2K bug’) (SSC 1999). In an interview with the authors, an SSC official noted that by March 1999, State Services Commission personnel, now closely involved with the governance of INCIS had formed the opinion that IBM could not ‘deliver the goods’ for the INCIS contract. They decided the best option was to halt the project, and negotiate a graceful exit. In May, the Treasurer, Bill Bitch notified Cabinet that IBM has informally advised officials ‘that it does not intend to complete Increment Two of INCIS due to the time and cost of completion..." (Birch 1999, 1). Investigations were then made into two alternatives to INCIS: PULSE, used by the Irish police, and VersaTerm, used by the Royal Canadian Mounted Police.

In June 1999, a Ministerial Group was established with a brief to review and monitor the project. This contained front-bench senior ministers including the

powerful ‘minister for everything’ Treasurer Bill Birch, the Minister of Finance Bill English, as well as the Ministers of Commerce, Police and Associate minister of State Services. The Chief executives of the Treasury, State Services Commission and the Department of Prime Minister and Cabinet, and the Police Commissioner, were required to oversee the INCIS and report to the ministerial group. There was intense media interest in the INCIS project at this stage, but public statements from the government and Police continued to indicate that INCIS would be continued. The Police Association chairman, Greg O’Conner, criticised INCIS, saying it ‘has not impacted on any police officers' lives’ and ‘so far, it's only being used by the intelligence people’ (Bell 1999, 24). The Justice and Law Reform Select Committee of the New Zealand parliament were also becoming increasingly concerned and requested that the Audit Office review the protect – a request the Office was unable to fulfil in totality due to some issues being sub judice (Waitai 1999).

*The Death of INCIS*

According to an interview with one contractor, IBM had threatened to withdraw as early as late 1997, and discussion about termination within the government goes back at least as far. As the Treasurer noted in May, IBM informally advised officials that it did not intend to complete increment 2 and the government was began canvassing its options in response (Birch 1999). However the INCIS project officially ended in early August 1999 when IBM advised the Police that it would not continue work on INCIS without renegotiating the contract to include further payment. The public response of the Police and Government was that IBM should continue work under the existing conditions and terms of payment. The Treasurer Bill Birch argued that since

there was a fixed-price contract, IBM should deliver the goods for this price. IBM then repudiated the contract on August 17th. The government publicly stated that IBM could not walk away from the contract. IBM, however, insisted that 'the goalposts have been moving since day one' and that it was owed 'a substantial amount of money' (Brown 1999, 1-1).

On 17 August 1999 the Attorney-General filed proceedings against IBM in the High Court at Wellington. The Crown sought judgement in relation to three causes of action and sought various forms of relief, including two sums over $3 million (excluding GST). A Statement of Defence and Counterclaim was then filed by IBM seeking $75 million and court costs in compensation for losses it claimed it sustained from the project. IBM maintained from Tokyo that they had 'met their contractual obligations [and] have done more than required. We are very proud of what we have already delivered which has resulted in a modernisation of police computer services (Beynen 1999, 1)'. One hundred and twenty five contractors working on the project were made redundant, while of the 25 IBM employees, between '10 and 20' were to stay on as 'part of the company's maintenance obligations [with] the rest "reassigned' within IBM' (Beynen 1999, 1). Subsequently, the government and IBM settled out of court. IBM paid the Crown $NZ25 million, while the Crown paid IBM $NZ18 million for work already completed (Evening Post 1999). The mainframe was sold at a reported price of $1 million, knocked down from the original cost of $7.6 million. Commissioner Peter Doone took early retirement after a controversy involving his partner, while deputy commissioner Barry Matthews left to take up a senior post in the Western Australia (Press 2000). The Police continued using the Wanganui computer.

An initial Commission of Inquiry was abandoned in favour of a Ministerial inquiry, headed by Dr Francis Small, which reported to the Minister of Justice in the newly elected Labour Government on 19 October 2000 (Small 2000). In April 2001, the Government indicated that it would accept all the recommendations from the report (Mallard 2001). The reports on the failure of INCIS led the State Services Commission (SSC) and other agencies to introduce new policies and requirements for the approval and monitoring of large IT projects (SSC 2001).

After the INCIS failure, Police needed substantial additional funding to pay for the project including a $94.6 million injection of funds during 2000. This included a $66 million write-down for computer hardware, software and network costs associated with the INCIS failure. The drain on the Police budget caused by INCIS led to buildings not being maintained and fleets of cars not being upgraded during 1996-98 (Hawkins 2001a; Hawkins 2001b). In the end, INCIS provided little more than a highly expensive e-mail system, and a number of terminals to the Wanganui computer.

In April 2001, Police began planning an organization-wide computer system, quickly dubbed ‘INCIS 2’ by the media (Pamatatau 2001). The Police now claimed to reject large scale IS projects, rather claiming developments should be ‘incremental, evolutionary and modular, acknowledging that there is no 'silver bullet' solution for Police IT requirements (Police 2001, 6).’

**Failure in Information Technology Systems**

Failure is a social construct and perceptions of what is and is not failure can vary between persons, and over time (Bovens and Hart 1996). Opinions differ to what extent failure is a normal part of public policy, or whether it is an unusual, if sometimes spectacular, event seized on by the media for the sake of eye-catching headlines (Bovens, Paul, and Peters 2001). What distinguishes IS failure from other failures in the public sector, however, is its overwhelming ubiquity. Indeed, while some writers might claim failure in IS development is unusual, the bulk of the research suggests that failure might even be the *norm*. As Mahaney and Lederer (1999, 291) note, 'because this problem has endured for three decades, many IS professionals have accepted failure as inevitable'. That these failures, both in the public and private sector, do not receive the media and other coverage that might be expected given the huge sums involved, says as much about the control of information and the 'spin' on stories, as it does about any 'reality' of failure.

Within IS circles there is some debate as to what constitutes failure or success and Bascarini notes that 'a standardized definition of project success does not exist, nor [is there] an accepted methodology for measuring it' (Bascarini 1999). Indeed, what is counted as failure 'depends on who you ask' and perceptions of success and failure may change over time (Kiel 1994; Larsen and Myers 1999). The Standish Group sees success in narrow terms if a project is delivered on time and on budget, with functions and features delivered as originally specified. Shenar et al (1999) argue there are four dimensions to IT success.

1. Project efficiency, which is the extent to which the project is completed on time and on budget.
2. Impact on the customer, measured by the extent to which the project meets its scope or functional requirements.
3. Business and direct success, which is the direct impact of the project on the organization and the degree of beneficial change that occurs because of the project.
4. Preparation for the future for the organization.

Bascarini simplifies these factors into two. First, 'project management success' as the projects conformity to specified time, cost and function requirements, and second, 'product success' as the effects of the final product and its fitness for the purpose (Bascarini 1999). Heeks and Bhatnagar (1999, 56) distinguish between total failure 'in which a proposed reform is never implemented or implemented but soon abandoned' and partial failure in 'which reform is implemented but has something wrong with it'. KPMG has defined 'runaway projects' to be those that overrun their projected budget or completion date by more than 30 percent, while others have proposed an overrun on budget or timeframe of 100 percent as a measure of failure (Cole 1995; Glass 1998). Larsen and Myers (1999, 399) suggest that 'success and failure can only be determined by considering the opinions of the stakeholders.' This approach has limitations however. Assessments are going to differ depending on the stakeholder, be they programmers, consultants, management or end users, and may change over time, as Larsen and Myers found, and as we have seen with IBM's response to the INCIS fiasco. This means that at some point someone will be making a judgement on the status of the project – and often this judgment will be dependent on the interpretation of events by a scholar or consultant, which may draw on, but be

quite in contrast to, the beliefs of various shareholders. In any event, on any of these definitions, the INCIS was a failure and more-or-less a total one. It achieved virtually none of its proposed functions, was faced with time and cost overruns, and ultimately abandoned.

*Why do Information System Projects Fail?*

The question arises why do IS projects fail? Heeks provides a checklist of Critical Failure Factors, seen in Table 1. In their compelling study of IT failures, IT journalists Collins and Bicknell provide an checklist of factors that point to failure (Collins and Bicknell 1997). These are outlined in Table 2. While useful, a factor approach has been critiqued by a number of writers. First, 'the factor approach tends to view implementation as a static process instead of a dynamic phenomenon, and ignores the potential for a factor to have varying levels of importance at different stages of the implementation process (Larsen and Myers 1999, 398)'. Second, the relationship between the factors is often unexplained (Ginzberg 1981; Lucas 1981). Indeed, the approach can assume that that each factor is an independent variable and underplays the interaction between them (Bussen and Myers 1997; Nandhakumar 1996a; Nandhakumar 1996b). Third, a number of studies have shown a lack of consistency in the importance of factors and few have been important in all cases (Kwon and Zmud 1987). Fourth, the factor approach is claimed, perhaps unfairly, to be overly mechanist while underplaying the importance of such things as organisational culture in development and the importance of the political, social and environmental context within and outside the organisation (Bussen and Myers 1997; Nandhakumar 1996a; Nandhakumar 1996b). This last criticism would be difficult to

sustain in relation to Heeks' critical factor approach, which explicitly takes account of such environmental, cultural and political factors.

Rather than simply ticking a checklist of factors, other accounts of IT failure have adopted and applied various theories of organisational and individual behaviour, often reflecting the then current management fad. What is called the interpretive approach sees humans as 'active makers of their physical and social reality' (Larsen and Myers 1999, 398) and not 'merely an inactive although problematic part of a system, something that can be optimised through selection, education and training' (Mourtisen and Bjorn-Andersen 1991, 312). The 'Progress research stream' literature has focussed on the relationships between IS developers and end-users and the effect of the IS on organisations (Kwon and Zmud 1987). Heeks, expanding on his Critical Failure Factors, has noted the noted that ISDs are 'social systems…rooted in a context of people and social structures' (Heeks and Bhatnagar 1999, 55).

*Controlling Failure Through a 'Learning Organisation'*

Other studies have seen IS failure as a problem of learning where organisations fail to learn from external and internal sources, and fail to moderate beliefs and behaviour in the face of failure, such as persisting in IS developments longs after they have proved to be unfeasible (Irani, Sharif, and Love 2001; Lyytinen and Robey 1999; Wastell 1999). Organizations fail to learn, it is claimed, because of limits imposed by such thing as information overload, high turnover of skilled staff, embedded ways of thinking, the drawing of strong conclusions from limited individual experiences and an inability (and lack of incentives) to draw lessons from previous failure (which are often forgotten in any event) (Lyytinen and Robey 1999). The separation of IS from

other units within a business and its overwhelming technological and engineering background can also isolate IT specialists from wider issues and learning. Over time, it is claimed, organizations 'accept and expect poor performance while creating organizational myths that perpetuate short-term optimization' (Lyytinen and Robey 1999,85). The high levels of stress and anxiety involved for participants in IS projects also undermine learning (Wastell 1999). Groups and individuals cope with this stress through 'defense-avoidance behavior patterns' such as reliance on organizational ritual, political infighting, and isolationism where groups develop a laager mentality and an inward looking, mutually-supporting and outwardly suspicious 'groupthink' ('t Hart 1994). These defenses work to avoid having to engage with the problems in the project, and face up to and learn from these problems (Wastell 1999). Failure then, it is claimed, will be reduced by creating incentives for organization and individuals to learn such as rewarding bearers of bad news and mistakes, providing a supportive environment for learning, integrating IS within the wider organization, and a broader focus of IS developers away from their mainly technical focus (Lyytinen and Robey 1999,85; Wastell 1999).

While it possibly provides some genuine insights, the 'learning organisation' literature upon which Lyytinen and Robey, and Wastell have drawn has been much critiqued. It has been seen as naive and utopian and as having questionable empirical foundations (Salaman 2001; Symon 2001). It has been seen as having a moral foundation that is at odds with the ethics actually prevalent within firms (Snell 2001). It is unclear as to what learning actually is and who (the organisation or the individual) is carrying out the learning (and sometimes the two are conflated in any event) (Popper and Lipshitz 2000). It underplays the barriers that exist to learning due

to the strong culture, hierarchy and rituals of organisations, and the 'paradigm', 'discourse' or belief systems, mostly external to the organisation, within which managers work and which rule out some options and constrain others (Salaman 2001). And, like any fad, it may already be losing the appeal it once had to consultants, scholars and practitioners (Symon 2001).

The question also arises how relevant some of the 'learning organization' literature is to explaining IS failures, particularly in the public sector. First, the high level of IT failures seems to suggest that while it would be nice if failure did lead to learning, or that there *would* be learning if just the right culture and organizational structure existed, there is little evidence for this occurring now or in the future. This is despite some of the organizational literature suggesting that a high-failure and high-risk industry such as IS industry should be one characterized by learning. One study argued that 'a high perceived likelihood of potentially costly but avoidable errors facilitates learning' (Popper and Lipshitz 2000, 292). This is because 'failure is an essential prerequisite for learning as it stimulates the sort of experimentation…advocated for sound policy development and organizational management (Sitkin 1992, 243). In contrast, Clarke and Perrow's (1999) analysis of failure led them to conclude that high-technology and high risk systems did not foster organizational learning. Plans supposedly to deal with failure, become 'fantasy documents', which are believed despite contrary experience, and serve to legitimate actions and provide comfort to management and clients, whether-or-not the organization has the ability to adapt to difficult situations. In some case, these 'plans' have contributed to the failure (Clarke and Perrow 1999).

Second, in some cases it is unclear what it is the organization should learn so as to avoid IT failure. There is no agreement on what Critical Factors or software development methodologies or management systems or latest management fad is effective in preventing IS failure. None has been particularly successful so far. Despite decades of development, there are still no reliable and accurate methods of estimating software project size or costs and no software development methodology that guarantees good results. Software estimation and project management techniques are reliant on the judgement of skilled individuals for success, and even the best can be wrong (Evans 2001). For example, Fenton (1997) found experienced managers were over 50 percent wrong in estimating software costs, and some software tools produced results that were incorrect by 200 percent. This was for completely specified projects, using experienced people and well-proven technology. Jacobson (1998, 354) found that the estimated project size at the beginning of a project 'may differ from the final size by a substantial percentage, say 50 percent.' Size was directly related to cost, and cost increases more quickly as project size increased.

Third, it is questionable how relevant some of the buzzwords of organizational learning such as 'thriving on uncertainty', 'discovery and reinvention', 'maintenance of a broad vision', 'market realignment', 'creative thought and requirement satisfaction', 'realignment of disruptive to creative technology', 'realizing the potential for change within the expectation of each shareholder' and so on (Brown and Eisenhardt 1998; Irani, Sharif, and Love 2001) are to rather staid and non-market driven government agencies, quite apart from what these buzzwords actually mean, and quite apart from the best efforts of managerialists and consultants to apply putative private sector management principles to the public sector. Whether or not a

government agency has the latest, fastest, gee-whizzist IS system or the then-most-popular 'learning organization' structure is not necessary going to affect its long-term viability, particularly if the agency is not competing in a market situation. However, its viability, or at least its ability to meet its objectives and carry out its functions, might be severely undermined in a period of fiscal constraint if millions of dollars are spent with little result.

Fourth, the literature particularly focuses on IS within a firm or an organization, and integrating that IS division or section to the wider needs of the organization. However, as we see in the case study, organizations, particularly government agencies in the age of NPM and contractualism, are often dependent on outside consultants to advise on IS development, and for large IT companies to develop and supply software and hardware. Failure might encourage learning, but it may be of a type not of great benefit to the purchaser. A consultancy company might well learn that advising proceeding with a large IS projects is well within its interests and guarantees a flow of income in the future, quite apart from the value of this IS project to the purchaser. It might also learn that whether their advice turns out to be good or not will have little relationship to its financial rewards then and in the future. It may well learn that advising what the management already thinks is a good idea, is enough to make them seem to be particularly good at their jobs and so be suitably rewarded. It might also continue to argue that new management structures or reorganizations will fix any problems that may arise. It is notable that consultancy reports on the INCIS project did not caution against IS as such, or the highly ambitious claims made for the INCIS system, but mainly about how the project and contract would be managed. Similarly, IT companies and their salesman might learn

that promising largely unachievable results from highly expensive IS projects is a good way to subsidize their software and hardware research and add to the company's profits, with little risk that contracts, however many pages they might run to, will be able to hold them to account. The learning organizational literature reflect what we argue is the pathological faddism of IS projects, which sees problems of failure solved simply by applying or developing the appropriate management skills and structures or 'fantasy plans'. Nor, as we will argue, is there any evidence that consultants, IT companies, public agencies or many practitioners and academics have learnt one of the key lessons of IT failure – that large and ambitious projects should be treated with great caution or avoided altogether.

*Project Escalation*

If the 'learning organisation' approach throws only a little light on why IS projects fail in such numbers are there other approaches that shed light on why large projects continue even after it is apparent they are failing? Much has been written on the escalation of software projects and 'run-away projects'. Various models have been proposed on why projects continue even when it seems obvious the project is a failure and it is only a question of throwing good money after bad. Keil, Mann, and Rai (2000) test four theoretical approaches to explain escalation behaviour: self-justification theory, prospect theory, agency theory, and approach avoidance theory. In self-justification theory, it is argued that managers continue their commitment to a project to justify earlier decisions, both to themselves and to others. In prospect theory, managers engage in risk seeking behaviour due to a choice between a sure loss – the sunk cost of the project – and possibility of a larger loss with at least some chance (however small) there will be a return (Kahneman and Tversky 1988).

Agency theory focuses on the problems faced by the principal (such as the manager or owner) of controlling an instrumentally rational agent (such as a programmer or IS developer and project manager) in a situation of information asymmetry and problems of monitoring where the agent may have more knowledge of the problems and an incentive to conceal them. In complex software developments it is also difficult to ascribe blame if and when projects do meet problems. Approach avoidance theory argues managers continue a project because the forces encouraging abandonment (restraining forces) are overpowered by the forces encouraging continuance (driving forces). In particular, what is called the completion effect – which is the nearness to the successful completion of the project - is a strong driving force. In IS development, this is particularly relevant due to the '90 percent completion' syndrome where the proportion of the completed project increases readily to where it is estimated to be 90 percent completed, whereafter it increases very slowly (Abel-Hamid 1988). In some cases, projects are reported to be 90 percent complete for half the duration of the project. In a survey of IT auditors, it was found that while all four explanations of IS escalation were statistically significant, the completion effect derived from the approach avoidance classified over 70 percent of runaway projects (Keil, Mann, and Rai 2000).

*Project Initiation*

Convincing accounts can be made of why IS projects are continued after they seem to be 'runaways.' However, we argue that what is missing from this picture is an explanation to why large IT projects are initiated. Despite the predominance of large IT failures, there is no evidence of fewer large and ambitious projects. Even after the INCIS debacle in New Zealand further large projects continued to be developed in the

New Zealand public sector, sometimes ignoring the regulatory regime that was developed in response to the INCIS and other disasters (Hosking 2002). Indeed, in October 2002, the government announced another large IS development in the Social Development Ministry at a projected cost of between $87 and $178 million, dwarfing even INCIS (Milne 2002, 3).

To explain why large and ambitious projects continue to be initiated we propose a model containing four pathological enthusiasms. Each enthusiasm is linked to a key player or group within public sector IT developments. First, idolisation where public officials 'use computers and are over-aware of IT's potential. They believe that IT can transform the business of government. The public sector becomes awash with IT driven reform projects, which place technology at the heart of the change process (Heeks and Davies 1999, 27)'. Second, technophilia or 'the myth of the technological fix' where 'the entire IS profession perpetuates the myth that better technology, and more of it, are the remedies for practical problems (Lyytinen and Robey 1999, 95).' Third, lomanism, drawing on Arthur Miller's archetypal salesman Willie Loman in the *Death of a Salesman*. Lomanism is the enthusiasm, feigned or genuine, that sales representatives and other employees develop for their company's products and skills, and that company's ability to develop new products and technologies, whatever the objections or questions put forward by potential and actual purchasers. Fourth, Managerial faddism. This is the tendency for consultants and managers to eagerly embrace the newest management fad, methodology or utterings of the Management Guru of the moment – whether this be such things as the learning organisation, knowledge management or New Public Management in the case of the public sector. It is reflected in the belief that most problems can be fixed or prevented,

and benefits created, by improving management structures along the lines of the new fad, with new IS projects often as a key element – as often seen in the Business Process Reengineering literature that seems to have influenced the police reorganisation that was carried out along with the INCIS project. It does not usually entail questioning the IS ambitions of management, but instead proposes how these might be better managed using this latest methodology or system and/or by simply employing better management. Together these four enthusiasms feed off and mutually reinforce each other, creating a strongly held belief that new and large IS projects will be a good idea. Doubters and sceptics can be portrayed as 'negative' 'Not Team Players', 'Not Helpful' or, particularly in a public sector influenced by NPM and economic models of behaviour such as public choice, as 'vested' or 'rent-seeking' interest groups, again to some extend seen in the response to critics of IT changes within the New Zealand police force. Together these pathologies make up the *Four Enthusiasms of IT Apocalypse* seen in Figure 1. When a project does enter problems, these four enthusiasms can also undermine attempts to curtail or abandon the project – a project can always be fixed with better management, or more technology or better programming.

*Technological Fixes and Managerial Faddism*

The INCIS project contained an unfortunate mix of technical and managerial faddism. The Police had a fairly well entrenched attitude that technology would solve all their problems – very much the classic 'idolisation' noted by Heeks. Indeed, SSC officials noted that police were 'carried away by the wonder of it all', while ex-contractors noted the Police's excessive confidence in IT, despite their limited experience of it.

The highly sophisticated functions required for INCIS had not been achieved elsewhere in the world and may not be for some time, and the 'architecture' of the project was unusual and complex. INCIS was a highly complex research project - a 'bleeding edge' development – IS jargon for complex and ambitious developments where the 'blood is on the floor'. That technical specifications were changed several times during the life of the project did not reduce this complexity.

If developing an innovative and large scale IS projects was not complex enough, a large scale reorganisation of police management structures was also carried out – a 'Business Process Reengineering' (BPR) [11] tied to the Community Policing Project known as Policing 2000. INCIS and Policing 2000 were initially planned as being intertwined, with Policing 2000 as 'the name of the program within which INCIS and other change and development projects are being integrated, planned and implemented' (Phillippson and Doone 1995). This Business Process Engineering, to use the Police jargon of the time:

> seeks a dramatic improvement in performance. It focuses an organisation on customer services and analyses processes in terms of value of the service to the customer. It develops a vision of future performance for each process, and eliminates, combines, simplifies or replaces activities, or whole processes, which are not adding optimum value. BPR uses technology, particularly IT, as an enabler of performance improvement. It relies on the introduction of rigorous performance measurement as a guide to both initial and ongoing performance improvements.
>
> The changes contemplated for Policing 2000 will be more demanding than Police have ever before attempted (Luxton 1995, Appendix A, 10-11).

While the report to the Cabinet State Sector committee stated in bold print that **'Policing 2000 is not about job cuts.'** (Luxton 1995, Appendix A, 9), it involved the 'downsizing' of 500 positions, although these were not ultimately carried through due to political pressure.

As the Police themselves later noted, Policing 2000 added to the complexity and difficulty of the project and so to delays experienced. In February 1996, the Deputy Commissioner of Police and Secretary of Treasury wrote to the Ministers of Police and Finance seeking an extension of time for reporting due to ' complexities inherent and the sequencing of events in applying business process re-engineering methodologies which are required to support new technology design' and that Police had 'broadened the scope of their work from primarily an operational focus in an INCIS solution to an organisation-wide business process re-engineering and a number of business and technology project solutions including INCIS (Small 2000, 48). When INCIS failed, the Police were left with an organisational structure which relied on a non-existent computer system. That the Police embraced one management fad and carried out a massive reorganisation of their organisation at the same time as developing a large IS does seem to be of questionable wisdom, but it is not unusual in IS failures (Collins and Bicknell 1997).

**The Impossibility of Control**

IS projects may be particularly difficult to control in the public sector. There are three issues here. First, the difficulty of monitoring of ISDs to try and keep them from going off the rails. Second, questions of accountability arise if and when the project

does go off the rails. Third, public sector ISDs must be managed in an environment subject to legislative change.

*Responsibility in Bureaucratic systems*

In a Westminster system such as New Zealand, ministers hold a vicarious responsibility for the decisions and omissions of their departments and the employees of their departments, in theory at least. That this vicarious responsibility, let alone the personal responsibility of the minister for his/her own actions, is not taken as seriously as some constitutional scholars would prefer, and may have been undermined somewhat by the doctrinaire application of NPM to the New Zealand public sector, has been much commented on (Goldfinch 1998; Gregory 1998). It is a principle that still has some force, however, at least amongst some voters and scholars. However, in complex IS projects that may last several years, there may be a number of ministers coming and going, as is the case of the INCIS project where there were four ministers, culminating in a Ministerial Group when things became too bad to ignore. These ministers may or may not be aware of the project and any problems it is facing, and so may not be in a position to ameliorate any of the effects. Nor in the age of NPM would ministers usually involve themselves in the operational matters of their departments until problems become too large and politically damaging to ignore. Because of these factors, in the case of failure, it may be difficult to hold one individual minister responsible, even if that minister did approve the original project. It might be easier to pin the blame on a particular government – as the Labour Government after 1999 has tried to do in the case of INCIS. However, if it is difficult to ascribe blame for dramatic disasters that have a seemingly simple cause-effect

relationship (Gregory 1998), it is vastly more difficult to hold ministers and governments to account for highly complex software and hardware development projects where it is demanding enough to explain what actually happened and why failure occurred, let alone who is responsible.

If conventions of ministerial responsibility provides little hope for accountability, let alone for the control of projects, could the chief executive, senior manager, or project sponsor be in a position to avoid project failure and be held to account if things do go wrong? This again will be difficult. The problem of complexity and blame-ascribing arises. It may be that it is beyond the power and expertise of the CE or manager to control the project, even if she attempted to do so. In the case of a manager being highly linked to the project itself, one might find problems already noted of self-justification, prospect, agency, 'keeping mum' and completion effects. This may possibly be seen in the INCIS failure where the Police Commissioner was highly identified, and identified himself, with the project, and continued to reassure outside monitoring authorities right until the last that the project was on track. For example, Doone wrote, in a letter to a magazine that 'less paperwork and streamlined procedures will follow with the introduction of new technology, including INCIS. The new systems are late but they are coming in (Doone 1997, 8-10). He was also a strong proponent of the new type of 'community policing' that was to be supported by the new IT systems, and was highly linked to its supposed benefits (Doone 1989). Similarly, the Project Manager Crewdson was an initiator of and strongly linked to the project and similarly assured doubters as to its status. He was also accused of not keeping enough distance between himself and the IBM suppliers (Justice and Law Reform Committee 1999). The problems of control within

the line hierarchy were further complicated by the unusual reporting requirements between Batchelor (Director of IT) and Crewdson (Project Manager) and the personality conflicts between the two.

Could front-line staff be a check on the empire building and ambitions of management and others when it come to developing large IS systems? Front-line staff, such as police in the INCIS project, might well be able to provide a 'reality check' on IS developers and management. However, widespread opposition to the INCIS project did not have any effect in containing it. In the unlikely event that the INCIS project was successful in achieving its technological aims, this hostility may have undermined the success of the system. Indeed, a leading factor that leads to computer failure is the reluctance or inability of end users to adapt to the new technology, or in some cases, where end-users actively subvert the computerisation process (Al-Gahtani and King 1999; Collins and Bicknell 1997). There was little effort put into convincing the front line police that the INCIS project would be in their benefit and there is evidence of great scepticism amongst front line police, both in relation to the INCIS project and to the Community Policing project with which it was heavily intertwined. Front line Police made their opposition to the restructuring process and Community Policing well known. Greg O'Conner, the head of the Police Association during most of the INCIS, claimed that the Community Policing Strategy had undermined the effectiveness of front line police, undervalued 'firm but fair police officers' respected by the criminal fraternity, led to the dominance of the police force by 'academics', used up valuable resources and reduced the overall effectiveness of the Police force in 'fighting crime'. Dave Wilkinson, an ex-policeman noted in

magazine interview that ‘if there's a pub fight a computer isn't going to stop you getting bottled’ (Chamberlain 1997, 39).

This problem of control within government agencies may be facilitated by the structures of bureaucratic organisations. It may be that government or business bureaucracies are particularly prone to difficulties of control in IT systems. Various critiques of bureaucratic structures have noted the tendencies of members to follow commands even if they are misguided, and for responsibility and initiative to be discouraged (Merton 1957). While bureaucratic structures can be highly effective in times of stability, they can lack the flexibility to adapt in periods of rapid change and uncertainty (Beetham 1996; Crozier 1964). Studies of bureaucracies have also noted that members can withhold and distort information to superiors when it is in their interests to do so, which is in accord with problems of ‘keeping mum’ found in IS failures (Crozier 1964). There may also be a tension between authority from expertise and authority from position, particularly in a highly complex fields as IS development where line management may be supervising people with highly specialist skills which management do not necessarily understand (Beetham 1996). Appointment may be made on seniority and the political behaviour of officials rather than simply merit, which again can be dangerous in highly complex specialist fields as IS development. As far as bureaucracies go, police forces are reasonably exemplary ones with strong hierarchical structures and culture, and with deference to superiors, to the extent that officers are given quasi-military ranks, and promotion often proceeds by seniority (Paoline, Myers, and Worden 2000). In such a culture, problems are not necessarily going to be brought to the attention of management or questions asked of the wisdom of the project, especially if the project is personally identified with the Police

Commissioner. Nor are 'front-line' grumbles going to be treated as carefully as they should, especially if the hierarchical cultures sits (however uneasily) with public choice and NPM notions of management-knows-best and the treatment of professional groups as rent-seeking interest groups. This culture may have clashed considerably with individualistic, heroic culture of the programmer and the faddish culture of the consultant and IT company employees (Figure 2).[12] Indeed, in one interview a contractor noted the rather difficult relationship between police line management and the programmers and that Police believed 'they [could] do anything', while Price Waterhouse audits also mention the difficult relationship, as noted. Unfortunately, in the era of NPM and the application of putative private sector management practises to the public sector, one of the aspects of bureaucracy that may have been of benefit in moderating IS failure has been undermined – that of conservatism and the suspicion of change. Some suspicion of change and of new and flashy IS innovations may have tempered some of the overblown expectations regarding the INCIS system. Instead, there may have been the worst of all worlds – a gee-whizz managerial NPM, and a heroic IS development culture, sitting atop of a largely traditional bureaucracy.

*Control through Contracts*

The growth of contractualism and New Public Management has partly been in response to perceived failings of the bureaucratic model. If large public or private bureaucracies have failings that make it difficult to control complex problems, then possibly a contractual type of relationship where-by outsourced IS experts are contracted to provide the appropriate services may provide a solution. However, there is considerable evidence that contracts are not effective in controlling projects and providing sanctions when IS project fail.

The New Zealand public sector is often seen as the most doctrinaire example of the application of contractualism to the public sector, heavily influenced by agency theory and transaction cost analysis (Goldfinch 1998). Indeed, the concern with contractual modes of management approaches fetishisation in the New Zealand public sector, with a vast array of public services and public service appointments provided for by contracts outside and within public sector agencies. Large contracts for IS projects are not unusual, nor is the naive belief that contracts will project purchasers against problems if and when they do arise – a belief that generally turns out to be mistaken (Collins and Bicknell 1997). However, there seems to be a particular reliance on the contract in the case of INCIS – whether this reflects the influences of the contractual culture of the New Zealand public service or the management style of Police is unclear. The Police's reliance on the contract was despite cautions raised regarding the adequacy of contract. For example, IBM and the Police proceeded to sign a fixed-price contract, in spite of warnings (including warnings in the Ernst and Young report they used for the business case) that they were not ready to do so (Ernst &Young 1993).

Difficulties in controlling the process were made difficult by problems in the design of the contract. Technology substitution clauses included in the INCIS contract served to void warranties on the software. IBM was happy to accommodate variations in the specification of INCIS, provided no warranty was required. The fixed-price contract was considered by the Police to be a guarantee that IBM would pay any overrun costs. However IBM, for their part, believed that it was politically

impossible for the Police to walk away from INCIS and that they could pass on extra development costs to the Police (Small 2000).

Changes in the legislative environment faced by the Police may have also undermined the contract. Crewdson, for example, claimed $14 million of the INCIS cost overruns were because of changes to the requirements of INCIS, such as legislative changes. While the INCIS contract had an 'off-ramp', whereby the project could be terminated at an early stage (required to be used between 29 September and 15 December 1995) with no fault found, this option was not exercised.

*Monitoring by Central Agencies*

Could central agencies monitor public sector projects and point out failure? They might not be particularly interested in doing so in the age of NPM and 'leaving managers to manage', at least until 'the IT hits the fan' (Iacovou 1999). In the case of New Zealand, the central computing body, Government Computing Services, was corporatised in 1987 and then 'privatised' in 1994 and there may not be the expertise or resources to adequately monitor other agencies, even within the central agencies such as the Treasury and the State Services Commission (SSC). Early in the 1990's there was little effective control and monitoring of IT project implementation by either the Treasury or the SSC (the agency responsible for overall management of the public sector). The decentralisation of the public sector under NPM inspired reforms further weakened this central control as departmental chief executives were given greater managerial autonomy and the role of the SSC was reduced. The Police were further removed from the control of the central agencies as they are not part of the core public service and are largely governed by their own act of Parliament, the Police

Act 1958. In December 1997, the Police INCIS project agreed to comply voluntarily with the monitoring regime, and sent copies of their internal and independent audit reports to the SSC for the December 1997 and March 1998 quarters. In May 1998 Cabinet directed that INCIS be subjected to the monitoring regime being conducted by the SSC, and on 12 June 1998, the SSC wrote to Police reiterating this.

After the central agencies became more actively involved in the monitoring of INICS, the Police consistently assured them that the project was progressing well. For example, during the period 1997/98, the Select Committee reported that most of 'the responses to us from the Police were positive in outlook and conveyed, particularly with regard to INCIS, an impression that everything was on track.' The Ministerial inquiry noted the 'INCIS Project was subject to the usual state sector reporting and approval processes, but the SSC were aware of failures by Police to report in accordance with the requirements of Cabinet (Small 2000, 186-7).' Police did not report at all to Cabinet between January 1996 and January 1998. Even when reporting, the Police were not always entirely co-operative with monitoring agencies or Parliament. As the select committee noted:

> ... issues of commercial sensitivity continued through the lifetime of the INCIS project. If we had accepted the Police's position, we would effectively have been accepting that no IT project in any department within our terms of reference could be subject to in-depth scrutiny by the committee (Waitai 1999).

While monitoring regimes have tightened in New Zealand since the INCIS and other disasters, they have not prevented further computer disasters and are unlikely to

do so in the future. Departments have often ignored them in any event (Hosking 2002). Given the problems of information and agency already mentioned, even if there was a will, resources and expertise available to monitor projects, there would still be difficulties. This would particularly be the case if the organisation being monitored is less than cooperative or cites such things as 'commercial sensitivity' - as with the New Zealand Police. In any event, the monitoring agencies only became important when it was obvious to all that the project was in severe difficulty and when it was largely too late to do anything about it. Decisive and early(ish) termination of the project when problems became apparent, while discussed, never became an actuality.

*Controls outside the Public Sector*

Employing external consultants may provide a check on the IS activities of public agencies, but will this also face the same problems of agency and informational limitations. Consultants may face an incentive to continue to support a project if their income is reliant on this project being initiated and continuing. If the consultant had earlier supported a project, she may also be prey to the same pressure of self-justification and completion effects. A consultant can also be open to the same pressures of groupthink, especially if he or she is strongly tied to the project. In the INCIS project, there was some concerns raised regarding aspects of the contract and management of the project, but none questioned the need for a large ISD. There may be cases where consultants have advised that large projects should not be attempted, or that they should be quickly abandoned as things go wrong before too much is spent,

but the literature does not seem to provide many examples. If and when the project fails, few consultants seem to have suffered ill-effects or been held responsible.

Could the IS suppliers themselves be a check on over ambitious projects? There are cases of IS companies informing purchasers that what they are suggesting is over ambitious, despite the incentives to agree to take on the project. Some writers on IT have alluded to the conservatism of IT engineers and their willingness to downplay what they can achieve (Glass 1999). Others however, have written of the heroic nature of programming culture where difficulties and possible failure are just further challenges to be solved by hugely talented programmers (Bronson 1999; Swanson 1988). Other note the particular technological focus of many IT and IS specialist, which may add to the culture clash and inattentiveness to problems of failure and appropriateness to the organisation. As Lyytinen and Robey (1999, 94) note:

> The profession of ISD is characterized by specialized training and circumscribed theorizing. Since the dawn of business computing, training in IS has meant 'computer training', and IS professionals remain technologists at heart. Unfortunately, a technologist's perspective does not encourage an accurate diagnosis of the role of computing in business strategy and operations.

Added to this heroic 'technophilia' is the 'lomanism' and managerial faddism of salespersons and IT company employees, who are often quite willing to agree with whatever the purchasers wish to purchase. In the case of INCIS, despite a number of failures already in the police force, there was never a question whether the large, radical and 'bleeding edge' INCIS-type project was the appropriate way to proceed. Indeed, no one in the police, the monitoring agencies or the external consultants, ever asked whether a large computerisation process was justified at all. IBM had little

incentive to disabuse the Police of the notion that IT can solve vast problems. On the other hand, in the INCIS case we find instances where even IBM cautioned against the achievability of proposed applications, but their cautions were disregarded by the Police, who pressed to continue. So the 'idolisation' of IT by the purchasers may even override cautions that are given by the suppliers.

*Reporting Problems*

Control, monitoring and ascribing blame is difficult in IS projects. The mis-reporting problems seen in INCIS have also been seen in a host of other IS failures. That members of organisations are reluctant to be the bearer of bad news is a well-reported phenomenon (Tesser and Rosen 1972). IS developments are no different, with bad news often under reported, concealed and sometimes even falsified in IS failures (Collins and Bicknell 1997; Heeks 1999; Smith, Keil, and Depledge 2001). Even internal IS auditors have been found to be reluctant to report problems for various organisational reasons including (sometimes justified) fears for their own future within the organisation (Keil and Robey 2001). Even when they have reported problems, these have often been ignored by their superiors (Keil and Robey 2001).

IS problems may be particularly susceptible to under or false reporting. First, 'even though they know an IS project is behind schedule, observers may lack confidence in their understanding of the actual extent of the trouble [as] most IS projects involve software development, and its intangible nature makes it difficult to estimate the proportion of work that has been completed (Smith, Keil, and Depledge

2001, 191).' Second, the 'scope of IS projects is often dynamic, and a projects boundaries may shift over time. While an observer may suspect that an IS project is in trouble, (s)he may not be completely sure and, therefore, his or her willingness to report …may be reduced (Smith, Keil, and Depledge 2001, 191)'. Third, there is a temptation for the project manager to simply 'tick the boxes' for project reporting, so as to back to the 'real work' of implementation. Management are frequently satisfied by this subterfuge, and are uninterested in the messy details of implementation. Management may be afraid of asking 'stupid' questions about the project for fear of losing prestige (Collins and Bicknell 1997).

This bring us to the conclusion of this section – not surprisingly, IS projects are extremely difficult to monitor. When things go wrong it is difficult to find those responsible and hold them to account. Nor do we believe that IS failure is simply a case of 'bad management' or stupidity, as much of the IS literature and some reports on INCIS imply. It may be that the complexity, uncertainty and risk in large IS developments, the complexity of personal relationships and the fallibility of humans, is such that by their very nature large IS projects are subject to a great probability of failure. We are also highly sceptical that some new management or technological silver bullet will greatly ameliorate this problem. Nor it is simply a question of finding super-managers immune to the failings found in other managers in IS failures. We are doubtful such manager-heroes exist. At best, the 'learning organisation' or clearer lines of accountability, or other management innovations, may make it easier for senior management to find out if a project is off the tracks. But even then, this bad news may not be wanted or 'heard' and may not lead to termination or modification of the project. Even crisis management may not work after it becomes apparent a project

is off-course. Changes to management structure as the problems in INCIS became obvious, including the establishment of ministerial and officials' committees, did not save the project. Management improvements will not necessarily stop, for the reasons outlined, ambitious and largely unachievable projects being initiated and large amounts of money being spent before the project's ultimate failure and abandonment. As we have already noted the problems of IS failure is much to with particular enthusiasms involved in the initiation and continuance of projects.

This leads us to the pessimistic conclusion that large IS projects are likely to fail, whatever the management or monitoring structure. Rather than continually seeking to control and moderate failure through new structures or monitoring regimes to report on project overruns – although these may be worthy aims in themselves – it may be better to avoid large and ambitious projects altogether and use already developed and proven technology to achieve modest aims.

**Pessimism as an IS Management Tool**

The INCIS failure may be a worst-case scenario in that it did most things wrong. In this it is an 'exemplary failure'. We have discussed aspects of this exemplary failure including, first, an extremely ambitious scope, developing new and unproven technology and attempting applications never achieved elsewhere. Second, increasing the complexity of the project by attempting organisational change at the same time and by changing technical specifications during the project development. Third, a naive faith in the enforceability of the contract between the police and IBM on the part of the police, and a belief in the contracts as a control device. Fourth, skill

deficits and management problems within the police, including tensions between members of the project. From the first, INCIS showed many of the key indicators of forthcoming failure such as: misreporting of results, timetable slippages, the non-delivery of applications and budget overruns, and tensions with the supposed users of the system – the front line police. Attempts to salvage the project by managerial reorganisation and the involvement of a greater range of experts, politicians and officials did not succeed.

It may be that the INCIS project is a unique and possibly tragic-comedic failure and so little can be learnt from it that will be of relevance to other public managers. What is particularly striking about INCIS, however, is the degree to which it repeats many of the same mistake found in other IS failures. There also seems little evidence that even the New Zealand public sector has learned much from the INCIS failure with large projects continuing and government enthusiasm for technology shifting its focus to ambitious claims made for 'E-government'. If our model of four enthusiasms of IS development describes how IS initiation might unfold, it suggests that large IS projects, and their subsequent failures, are destined to be with us for a while yet.

What then is to be done? Much of the writing on IS failure suffers from what Oakeshott (1962) might term 'rationalism', that is, a belief that there is some 'technique' that can be applied to IS developments that will fix them once and for all. That failure is so common still is because that right technique – a new programming style, a new management fad, a new consultancy template or whatever – has not been

discovered yet. Or if it has, it has not yet been applied. In the face of such optimism, and the four enthusiasms of ISD we have outlined, we suggest a pessimism when it comes to IS development. This is a belief that we do not fully understand the processes involved in IS developments, that their complexity makes them difficult if not impossible to control and that large IS development are likely to fail. Rather than simply a technical exercise of software engineering, the application of 'management science' and the talents of brilliant managers, or the bringing-in of highly skilled consultants, or even just some healthy combination of all of these, IS developments in the public sector are a potent and dangerous mixture of highly challenging technical problems, the frailties of humans and management systems, personality and other conflicts, problems of agency and information, legislative instability, and clashes of cultures between public servants, software developers, consultants and salesman and their respective organisations, amongst other things. If one thing characterises large IS developments, it is this incredible complexity. That these developments are often combined with other large-scale re-organisations, and that technical and other specification changes are sometimes made during the development process, only compounds this complexity. We do not believe that for the foreseeable future that some technique or techniques will be able to manage this complexity. Indeed, as expectations continue to grow regarding IT and IS, it may be that any improvements made in 'techniques' will be outpaced by the increasing demands made by complexity on all-too-human managers, public servants, software designers and other members of the IS industry.

Does this pessimism, this expectation of failure, imply an abandonment of IS development? In some case, yes. In the INCIS case, pessimism would have

hopefully prevented the project initiation and potentially saved $NZ100 million. This could have been spent more productively on the upgrading of police cars and buildings or 'fighting crime'. The Police could have continued using the clunky and outdated Wanganui computer for a few more years, possibly without great loss, which is what happened anyway. If the billions that have been poured away on IS developments in public sectors for no benefit, or even for systems less effective than their predecessors, had instead been spent on such prosaic things as schools, decent public transport and so on, with the large IS projects never actually initiated, we are prepared to go out on a limb and say that this would have been a good thing. This is dramatically underlined when a number of large IS failures have occurred in developing countries that are unable or unwilling to supply even the most basic public goods to their citizens.

Does pessimism imply that all technological advancement and IS developments should be abandoned and that we can do no better than we are doing now? Critics of philosophical pessimism suggest that it would – that pessimism is the 'enemy of hope' (Tallis 1997). However, even Oakeshott, who is often identified with philosophical pessimism, is reluctant to embrace an all-or-nothing approach. He criticises Hayek's *Road to Serfdom* for that very reason, seeing Hayek's total rejection of planning as just another ideology (Oakeshott 1962, 21). In this case the pessimism we are advocating is not a 'technological nihilism' a belief that all is hopeless, but simply a rejection of the enthusiasms of IS development, and a belief that large IS projects will usually not deliver their claimed benefits and will be nearly impossible to control and prevent from failing. This is not to say that small, modest and proven technological developments could not be of some benefit to the public sector.

How would this pessimism work in practice? At its most basic level, it raises the question whether new IS developments are of benefit at all. In the 'black box' of public management decision-making, it is often the solution – which might be restructuring along NPM lines or investment in IS or whatever - that is thought of first. The problem that this solution is to solve often comes after, or not at all. If the first step then, is to ask what is to be achieved and what problem (and there should really be a problem) is to be solved, the next question becomes: can we solve this problem without investment in further IS? Can some minor adjustment to current systems of management or IS deliver benefits without great costs and great disruption? If the costs, uncertainties and risks of change are great, do they potentially outweigh the costs and difficulties of continuing with the way things are already done?

If the decision is made to proceed with some ISD, then the question becomes how can this be done with the least disruption and the least cost, and with the least risk and uncertainty. The wrong answer would be to decide to invest in a high-risk, highly ambitious 'bleeding edge' large development which has a very high probability of failure, such as INCIS. A more sensible solution might be to examine what is currently working in the market place and try to buy something off-the-shelf that can be demonstrated to work. However, it would not do to buy a system that did not fit the organisation's needs, and then adapt this to particular legislative and organisational conditions. Once adaptations are attempted on an existing system, however well it might work in its home country or public sector, the probability of failure again becomes large (Collins and Bicknell 1997; Heeks 1999). If a system is

not in existence anywhere else, then the question again should be asked again, are the expectations held for ISD too high? If there is not a suitable off-the-shelf system that can be purchased, or one that approaches the organisation's 'needs', can expectations be scaled back to what does exist, or can the organisation get by without further ISD, at least until the technology improves? If the Police had asked these questions when considering INCIS, this would have increased the probability of success. In the public sector, a few years longer with an obsolete system is not going to be the end of the world – more-or-less functional is better than no function at all - and in most cases won't make much of a perceivable difference. The Police's continuing use of the Wanganui Computer has not led to the sky falling in, or an explosion of crime, or much of a difference at all for the outsider looking in. If the answer is still that ISD is needed, then, and only then, should ISD be considered.

Once the decision is made to proceed towards an ISD, then again pessimism should be the guiding principle. Aim small. Be modest about what can be achieved by ISDs. Be risk adverse. Expect problems. Assume the promises and enthusiasms of internal IS people, salespeople, consultants, management gurus, technicians and software engineers are unlikely to be worth much when a system fails, nor will any contract, even if it runs to thousands of pages. Believe that developments will work only when they can be shown to work. Realise that clashes of culture and the complexities of ISDs, make control and monitoring of projects almost impossible. Accept that there is no reason to believe that the current or proposed ISDs can better avoid the problems that have plagued all other ISDs for decades, or that current managers and programmers are somehow superior to those that have failed in the past. If there is to be restructuring of the organisation, this should not be tied to the ISD, but

carried out separately and before. It is unwise to increase complexity by changing specifications during the development. Be prepared to terminate the development if cost overruns, delays or non-delivery become apparent, despite claims it 'is almost there' or 'it will be alright on the night' (Collins and Bicknell 1997). The system, if it does work, is unlikely to lead to huge job savings, or even cost savings in the short term, and there may be a loss of productivity until staff becomes used to its idiosyncrasies. Excluding front line staff from development, while it might fit with the management fashion of the time, is also a high-risk strategy, and they might undermine the system even if it does work.

Once partial solution noted by the ministerial inquiry into INCIS and taken up the SSC is the recommendation that IS projects be broken into 'modules.' SSC Officials recommended in an interview that these be modules of one year or $5 million. If the system modules provide useful functions on their own, then the loss of other parts of the system is not so damaging to the project outcome – 'at least you've got something for your money'. An additional safety net could be to concentrate on linking small modules of an IT project to small chunks of an IT budget, with safeguards against transferring extra funds to unsuccessful modules.[13]

In sum, ISD is a minefield. Rather than believing there is a simple way of crossing this minefield, it may be better to not cross it at all, or to make this minefield as simple and small as possible and reduce its complexity and scope. Above all, it is best to approach this minefield suspiciously, sceptically and pessimistically, only then might the damage (and there will always be damage) be reduced.

Table 1

**CRITICAL FAILURE FACTORS IN IS DISASTERS**[1]

| **Factor** | **Description** | **Factor** | **Description** |
|---|---|---|---|
| *Information* | Information and data inadequacies | *Cultural* | Clashes with national/local culture |
| *Technical* | Problems with IT such as incompatibility across agencies | *Structural* | IS clashes with organisational and/or management structures |
| *People* | Lack of staff with sufficient training, skills or inclination to handle or develop IT | *Strategic* | IS not coordinated across different agencies or divisions |
| *Management* | Lack of management skills, knowledge and training | *Political* | Political infighting derails project |
| *Process* | Processes are inadequate to integrate community or channel relevant information | *Environmental* | Factors outside the organisation disrupt project |

1. Source: Heeks and Bhatnagar (1999)

Table 2

**COLLINS AND BICKNELL'S TEN POINTERS TO IS FAILURE**

- A tendency to be overambitious
- A feeling among computer managers that they know it all and cannot admit when they don't.
- A belief among the entire project team that computerisation must be a good thing, and to suspect otherwise is an Orwellian though-crime.
- A chief executive who is in the best position to judge a computer project because he knows nothing about computers but fails to intervene – because he knows nothing about computers.
- A readiness to accept it'll-be-all-right-on-the-night assurance from suppliers – assurance that suppliers studiously avoid writing down.
- An over reliance on consultants, who, like some vets, may have a financial interest in prolonging ills.
- An avoidance of cheap, proven, off-the-shelf packages in favour of costly, unproven, custom-built software; or worse, the tailoring of a standard proven package.
- An unwillingness by middle and senior management to impart bad news to the board – mainly because the board will make known its resentment of anyone who tries.
- The buck stops nowhere.
- A mistaken belief that the contract makes it easy to sue the supplier if it all goes wrong.

1. Source: This is quoted from Collins and Bicknell (1997, 15).

Figure 1
**The Four Enthusiasms of IS Failure**

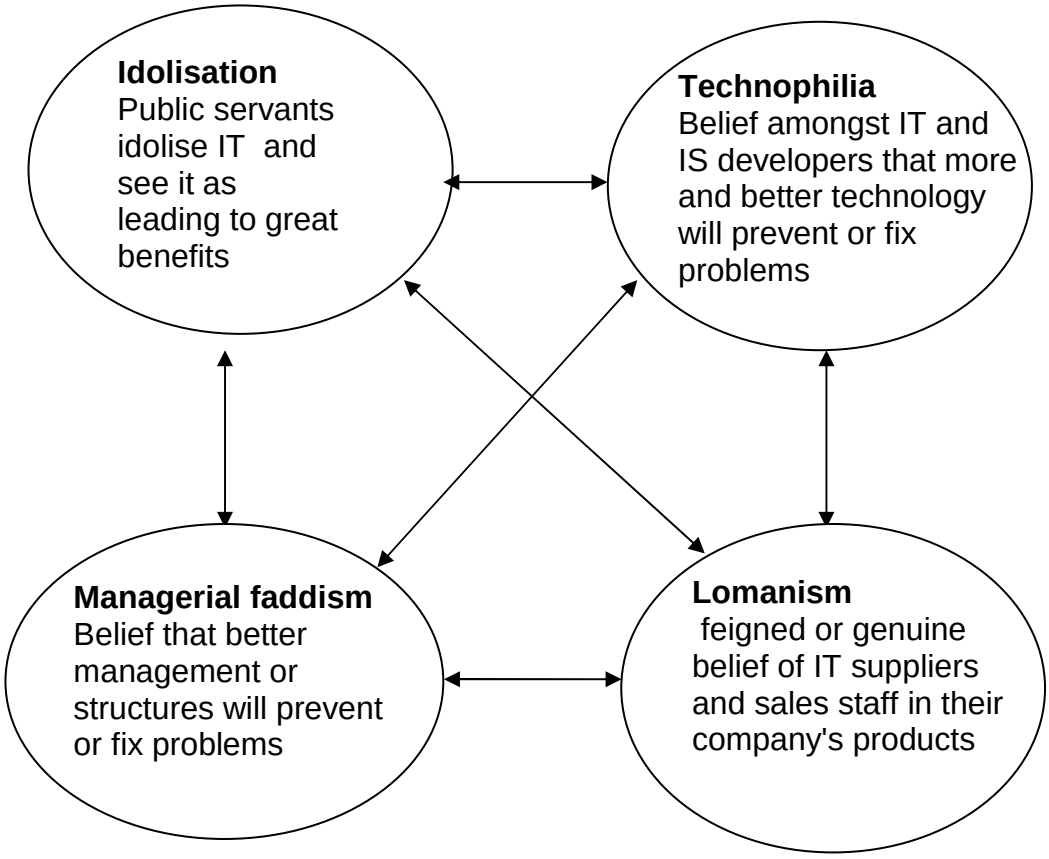
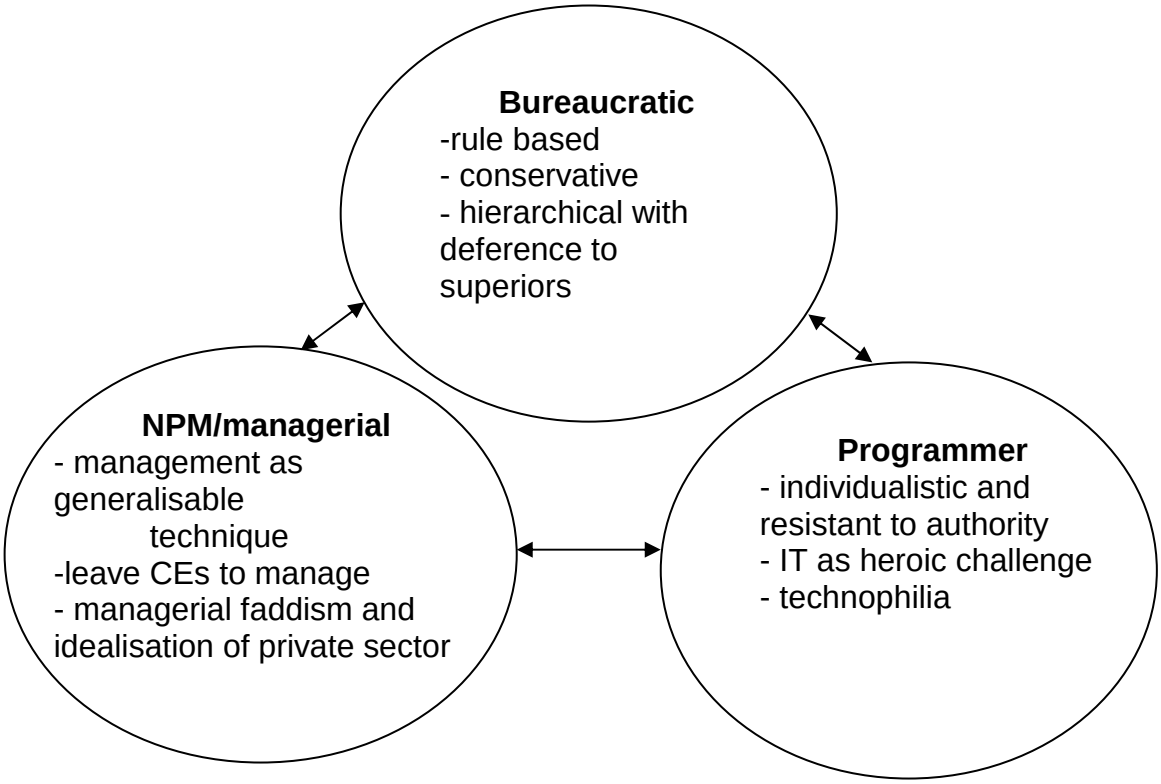


Figure 2
**Culture Clashes in Public Sector IS Developments**



*References*


Abel-Hamid, T. K. 1988. Understanding the '90% Syndrome' in Software Project Management: A Simulation-Based Study. *The Journal of Systems and Software* 8 (4):319-330.

Al-Gahtani, S. S., and M. King. 1999. Attitudes, satisfaction and usage: factors contributing to each in the acceptance of information technology. *Behaviour & Information Technology* 18 (4):277-297.

Bascarini, D. 1999. The logical framework for defining project success. *Project Management Journal* 30 (4):25-32.

Beetham, David. 1996. *Bureaucracy*. 2nd ed. Minneapolis: University of Minnesota Press.

Bell, Stephen. 1999. Police chairman admits INCIS makes no difference to coppers on the beat. *The Independent*, 9 June 1999, 24.

Beynen, Martin van. 1999. Legal battle looms over INCIS affair. *The Press* August 10:1.

Birch, Rt Hon W. F. 1999. Memorandum for Cabinet. INCIS Negotiating Strategy. 27 May. Obtained Under the Official Information Act 1982.

Bovens, Mark, and Paul 't Hart. 1996. *Understanding Policy Fiascoes*. New Brunswick and London: Transaction Publishers.

Bovens, Mark, 't Hart Paul, and B. Guy Peters, eds. 2001. *Success and Failure in Public Governance*. Cheltenham: Edward Elgar.

Bronson, Po. 1999. *The Nudist on the Late Shift and other Tales of Silicon Valley*. London: Vintage UK Random House.

Brown, Russell. 1999. 175 jobs to go along with INCIS. *Computerworld NZ*, Aug 10, 1999.

Brown, S. L., and K. M. Eisenhardt. 1998. *Competing on the Edge: Strategy as Structured Chaos*. Boston, MA: Harvard Business School Press.

Bussen, W., and M. D. Myers. 1997. Executive information system failure: A New Zealand case study. *Journal of Information Technology* 12 (2):145-153.

Chamberlain, Jenny. 1997. NZPD Blues: Can Cops Cope? *North and South*, October 1997, 34-52.

Clarke, Lee, and Charles Perrow. 1999. Prosaic organizational failure. In *When things go wrong: Organizational failures and breakdowns*, edited by H. K. Anheier. Thousand Oaks, CA, US: Sage Publications Inc.

Cole, A. 1995. Runaway Projects: Cause and Effects. *Software World (UK)* 26 (3):3-5.

Collins, Tony, and David Bicknell. 1997. *Crash, Ten easy ways to avoid a computer disaster*: Simon & Schuster.

Crewdson, T. 1995. INCIS Project Status Report. SSC archive L-3-21/5, 30 June. Obtained under the Official Information Act.

Crewdson, T. 1996. INCIS Status Report. SSC archive L-3-21/4, 31 March. Obtained under the Official Information Act.

Crozier, Michel. 1964. *The bureaucratic phenomenon*. Chicago: University of Chicago Press.

Davenport, T. H. 1996. Why reengineering failed: the fad that forgot people. *Fast Company, Premier Issue*: 70-74.

Doone, Peter. 1989. Potential Impacts of Community Policing on Criminal Investigation Strategies. In *Effectiveness and Change in Policing*, edited by W. a. C. Young, Neil. Wellington, NZ: Institute of Criminology, Victoria University.

Doone, Peter. 1997. Letter to the Editor. *North and South.*

Doone, Peter. 1998. Letter to the Editor. *Evening Post*. 25 February.

Doone, Peter. 1999. Letter to Patricia Schnauer, Deputy chairperson, Justice and Law Reform Committee, 28 September. Obtained under the Official Information Act 1982.

Economist, The. 2002. The health service's IT Problem. *The Economist*. October 19th, 51-2.

Ernst &Young. 1993. Report on Review of INCIS Project. Obtained under the Official Information Act.

Espiner, Colin. 2000. Failure to see IT signs cost Govt - expert. *The Press* May 5:3.

Evening Post, The. 1999. Editorial. *Evening Post. October 28.* : 4.

Fisk, C. 1993. Treasury InterOffice memo from Clement Fisk to Michael Moriarty Quality of Police Financial Management. March 4. SSC archive L-3-21/13. Obtained under the Official Information Act.

Galliers, R. D., and S. Newell. 2000. Back to the Future: From Knowledge Management to Data Management Working Paper Series 92. London: LSE, Department of Information Systems.

Ginzberg, M. J. 1981. Key recurrent issues in the MIS implementation process. *MIS Quarterly* 5:47-59.

Glass, R. L. 1998. Software Runaways - Some Surprising Findings. *The DATABASE for Advances in Information Systems* 28 (3):16-19.

Glass, Robert. 1999. Evolving a New Theory of Project Success. *Communications of the ACM* 42 (11):17-19.

Goldfinch, Shaun. 1998. Evaluating Public Sector Reform in New Zealand: Have the Benefits Been Oversold? *Asian Journal of Public Administration* 20 (2):203-232.

Gregory, Robert. 1998. Country Report. A New Zealand Tragedy: Problems of Political Responsibility. *Governance* 11 (2):231-240.

Hammer, M. 1990. Reengineering Work: don't automate, obliterate. *Harvard Business Review* July-August: 104-112.

Hawkins, George. 2001a. $13.2 (ex GST) Million Police Vehicle Package Announced. Ministerial press release.

Hawkins, George. 2001b. $60 million to address years of property neglect. Ministerial press release.

Heeks, Richard, ed. 1999. *Reinventing Government in the Information Age*. 2002 ed. 3 vols. Vol. 1, *Research in Information Technology and Society*: Routledge.

Heeks, Richard. 2002. Failure, Success and Improvisation of Information System Projects in Developing Countries. Manchester: Institute for Development Policy and Management.

Heeks, Richard, and Subhash Bhatnagar. 1999. Understanding success and failure in information age reform. In *Reinventing Government in the Information Age*, edited by R. Heeks. London and New York: Routledge.

Heeks, Richard, and Anne Davies. 1999. Different Approaches to information age reform. In *Reinventing Government in the Information Age*, edited by R. Heeks. London and New York: Routledge.

Hosking, Robert. 2002. ACC yet to explain its $173 million IT blowout. *National Business Review*, 8 Feb, 2002, 10-11.

Iacovou, Charalambous. 1999. The IPACS Project: when IT hits the fan. *Journal of Information Technology* 14:267-275.

Irani, Z., A. M. Sharif, and P. E. D. Love. 2001. Transforming failure into success through organisational learning: an analysis of a manufacturing information system. *European Journal of Information Systems* 10 (1):55-66.

Jackson, Randal. 1998. INCIS: Has it had a bum rap? , Apr 18, 1998.

James, G. 1997. IT fiascoes...and how to avoid them. *Datamation* November: 84-88.

Justice and Law Reform Committee. 1999. Inquiry into CARD and INCIS. Transcript of Evidence from Greg Batchelor as adopted on 8 September 1999. Obtained under Official Information Act 1982.

Kahneman, Daniel, and Amos Tversky. 1988. Prospect theory: An analysis of decision under risk. In *Decision, probability, and utility: Selected readings.*, edited by P. S. Gaerdenfors, Nils Eric.

Keil, M., J. Mann, and A. Rai. 2000. Why software projects escalate: An empirical analysis and test of four theoretical models. *MIS Quarterly* 24 (4):631-664.

Keil, Mark, and Daniel Robey. 2001. Blowing the Whistle on Troubled Software Projects. *Communications of the ACM* 44 (4):87-93.

Kiel, M. 1994. Managing IT projects for success: re-engineering of better project management. In *ICIS Panel Discussion.* Vancouver, 16 December.

Korac-Boisvert, N., and A. Kouzmin. 1995. Transcending soft-core IT disasters in public sector organizations. *Information Infrastructure and Policy* 4 (2):131-61.

Kwon, T. H., and R. W. Zmud. 1987. Unifying the fragmented models of information systems implementation. In *Critical Issues in Information Systems Research*, edited by R. J. Bolland and R. A. Hirscheim. New York: Wiley.

Larsen, M., and M. Myers. 1999. When success turns to failure: a package-driven process re-engineering project in the financial services industry. *Journal of Strategic Information Systems* 8 (4):395-417.

Lucas, H. 1981. *Implementation: the key to successful information systems.* New York: Columbia University Press.

Luxton, John. 1995. Integrated National Crime Information System. Report to Cabinet State Sector Committee, August. Obtained under the Official Information Act 1982.

Lyytinen, K., and D. Robey. 1999. Learning failure in information systems development. *Information Systems Journal* 9 (2):85-101.

Mahaney, Robert, and Albert Lederer. 1999. Runaway Information System Projects and Escalating Commitment. *SIGCPR '99*:291-296.

Mallard, Trevor. 2000. Government to sell INCIS mainframe. Ministerial Press Release by state Services Minister Trevor Mallard.

Matthews, B. 1996. Letter to the Office Solicitor of the SSC, D J Bradshaw. SSC archive L-3-21/14. 14 October. Obtained under the Official Information Act 1982.

Matthews, B. 1998. Facsimile Message from Barry Mathews to Brendan Kelly, SSC. May 14. Obtained under the Official Information Act 1982.

Matthews, B. 1999. INCIS Status Report to the end of December 1998. January 11. SSC archive L-3-21/39. Obtained under the Official Information Act 1982.

Merton, R. K. 1957. *Social Theory and Social Structure*. New York: Free Press.

Milne, Jonathan. 2002. Computer upgrade to cost ministry $178m. *The Press.* October 29: 3.

Minister of Finance, Minister of Police and Associate Treasurer (4/3/98). Bilateral Minute from the

Ministers of Finance, Police and the Associate Treasurer re 1998 Police Budget. SSC archive L-3-

21/16, obtained under the Official Information Act.

Mourtisen, J., and N. Bjorn-Andersen. 1991. Understanding third wave information systems. In *Computerization and Controversy*, edited by C. Dunlop and R. Kling. San Diego: Academic Press.

Nandhakumar, J. 1996a. Design-for success? Critical success factors in executive information systems development. *European Journal of Information Systems* 5 (1):62-72.

Nandhakumar, J. 1996b. Executive information system development: A case study of a manufacturing company. *Journal of Information Technology* 11 (3): 199-209.

Oakeshott, Michael Joseph. 1962. *Rationalism in politics, and other essays*. London: Methuen & Co.

Pamatatau, Richard. 2001. Police brief companies on building "Incis 2". *NZ Infotech Weekly*, 17 April, 2001, 1.

Phillipson, Ross and Doone, Peter. 1995. INCIS: Determining timing of the split of benefits. Letter to Minister of Police and Minister of Finance. 5 December. Obtained under the Official Information Act 1982.

Paoline, Eugene- A., III, Stephanie- M. Myers, and Robert- E. Worden. 2000. Police Culture, Individualism, and Community Policing: Evidence from Two Police Departments. *Justice Quarterly* 17 (3): 575-605.

Popper, M., and R. Lipshitz. 2000. Organizational learning - Mechanisms, culture, and feasibility. *Management Learning* 31 (2): 181-196.

Police, The New Zealand. 2001. National Strategy for Police Information and Technology Systems 2001-4. 20 April. Wellington: New Zealand Police

Press, The. 2000. Discord led to Incis bungle, says report. *The Press*, 18 November: 3.

Price Waterhouse. 1996. NZ Police INCIS Project Internal Audit. Obtained under the Official Information Act 1982: Price Waterhouse.

Price Waterhouse Coopers 1997. INCIS Project Internal Audit Quarterly Report, 30/6/97. Obtained under the Official Information Act.

Provost, L. (1998). SSC document S/3/79, INCIS Project - Options for strengthening. 27 July. SSC archive L-3-21/18. Obtained under the Official Information Act.

Rapley, J. 1997. SSC memorandum re Police INCIS project - risks. SSC archive L-3-21/17. 28 February. Obtained under the Official Information Act.

Salaman, Graeme. 2001. A response to Snell. The learning Organisation: Fact or Fiction? *Human Relations* 54 (3): 319-342.

Sapphire Technology Ltd. 1994. Report on INCIS.

Secretary for the Treasury. 1997a. Treasury document GD/33/0, letter from the Secretary for the Treasury to Police Commissioner Peter Doone. 27 February. SSC archive L-3-21/17. Obtained under the Official Information Act.

Secretary for the Treasury. 1997b. Treasury Document T97C/502 Letter from the secretary for the Treasury to the Treasurer and the Minister of Finance. 11 March. SSC archive L-3-21/7. Obtained under the Official Information Act.

Shenar, A.J., O. Levy, and D. Dvir. 1999. Mapping the dimensions of project success. *Project Management Journal* 28 (2):5-13.

SIMPL/NZIER. 2000. Information technology projects: Performance of the New Zealand public sector in performance. Report to the Department of the Prime Minister and Cabinet. Wellington: The SIMPL Group and New Zealand Institute of Economic Research (INC).

Sitkin, S. B. 1992. Learning Through Failure: The Strategy of Small Losses. *Research in Organizational Behaviour* 14:231-66.

Shennan, M. 1999. INCIS: Response to Andersen Consulting Advice. Treasury document GD/33/6/1. 12 March. SSC archive L-3-21/23. Obtained under the Official Information Act.

Small, Francis. 2000. Ministerial Inquiry into INCIS. Wellington.

Smith, H. J., M. Keil, and G. Depledge. 2001. Keeping mum as the project goes under: Toward an explanatory model. *Journal of Management Information Systems* 18 (2):189-227.

Snell, R. S. 2001. Moral foundations of the learning organization. *Human Relations* 54 (3):319-342.

Soar, Jeffrey. 1999. Gibraltar Review of Police I & T costs. Letter to Peter Doone, February 11. Obtained under the Official Information Act 1982.

SSC. 1999. Justice Sector - Y2K Issues: Report to Cabinet. Wellington, State Services Commission.

SSC. *Guidelines for Managing and Monitoring Major IT Projects* [WWW]. State Services Commission and Treasury, August 2001. Available from http://www.ssc.govt.nz/documents/iguidelines/guidelines.html.

Swanson, E. B. 1988. *Information System Implementation: Bridging the Gap Between Designing and Implementation*. Henley-on-Thames: Alfred Waller.

Symon, Graham. 2001. Beyond the Learning Organisation: Book Review. *Management Learning* 32 (2).

Tallis, Raymond. 1997. *Enemies of hope: a critique of contemporary pessimism*. New York: St. Martin's Press.

Tesser, A., and S. Rosen. 1972. Fear of negative evaluation and the reluctance to transmit bad news. *Journal of Communication* 22 (2): 124-41.

Treasury, The. 1999. Ad Hoc Minister's Meeting on INCIS. GD/33/6/1 T99C/359. Letter to the Treasurer and Minister of Finance. Obtained under the Official Information Act 1982.

't Hart, Paul. 1994. *Groupthink in Government: A Study of Small Groups and Policy Failure*. Baltimore: John Hopkins UP.

Waitai, Rana. 1999. Inquiry into CARD and INCIS: Justice and Law Reform Committee.

Wastell, D. G. 1999. Learning dysfunctions in information systems development: Overcoming the social defences with transitional objects. *MIS Quarterly* 23 (4): 581-600.

Wilcocks, L. 1994. Managing information systems in UK public administration: issues and prospects. *Public Administration* 72 (Spring):13-32.

Williamson, Hon. Maurice. 1993. Meeting between Hon Maurice Williamson and Police commissioner re: the new Police Computer System INSYS. 15 September. Obtained under the Official Information Act 1982.

Williamson, Hon. Maurice. 1994. Integrated National Crime Investigation System (INCIS). Letter to Hon John Luxton, Minister of Police. 21 February. Obtained under the Official Information Act 1982.

---

*Notes*

[1] Information System (IS) is a computer system combined with the organisation and personnel to (hopefully) produce useful output and accomplish organisational goals, as opposed to information technology (IT) which is a general term for computers, networking and software used in an information system.

[2] The 1996/7 operating budget for the Police was $NZ783.920 million, and for 1997/8 it was $NZ789.961 million, including an additional $NZ20.802 million approved by Cabinet after the 1997/8 budget round (Doone 1998).

[3] The report also noted that 'IBM has not been as successful in the applications delivery role as in the delivery of the IBM infrastructure and Police need to pay considerable attention to the effective project management and the necessary transfer of skills to in house staff (Ernst & Young 1993, 10).'

[4] On 21 Feb 1994, Williamson (1994) wrote to the Minister of Police, John Luxton and noted

> I consider the Police have opted for a higher risk solution than that which might have been provided by an international standard solution. Overall, based on the assurances given, it would appear that the contractual obligations on the vendor are strong enough to minimise the risks involved...

[5] The Police reinterpreted the external reports on the project in a more positive light than they were intended, disregarding the few cautions that were raised. The business case used as one of the main supporting documents a report by Ernst and Young (1993), which had been supportive of the INCIS proposal in an earlier version, when the technical specifications had been somewhat different. The rest of the report sounded a number of warnings that the Police were not ready to proceed to contract and that there were a number of critical issues to address. However, the upbeat executive summary of the Ernst and Young was still included in the INCIS business case. As the Ministerial Inquiry commented:

> given its [the contract's] inadequacies, why was it accepted? Presumably neither the Cabinet nor its advisers queried it sufficiently. ... It would seem, however, that searching questions were not asked with regard to risks, despite the awareness of some elements of risk evidenced by the Cabinet minutes approving the INCIS Project (Small 2000, 144).

[6] The Small report noted the expected efficiency benefits as $517 million over 8 years or $303 million net present value.

[7] Request for Proposal (RFP) and Request for Tender (RFT) are stages in the standard process when contracting for goods and services. The difference is that the response to an RFT requires a Tender with a firm proposal and costings.

[8] Doone claims that the report was further modified to take into account Batchelor's concerns and that the Andersen review of the project was also in response to these concerns. Batchelor had left the Police force by the time the report was delivered.

[9] Crewdson also stated: "Project management is now proceeding on the assumption that the Government will not be requiring Police to reduce it's capital baseline by an amount equivalent to 540 staff and that the attrition programme is cancelled."

[10] The distributed client-server approach to large software systems is still a complicated and difficult design method to use. It requires the co-ordination of, potentially, hundreds of different software applications and databases on physically separate computers. Compare this with the centralized and well-tried three-tier approach, where a few large central servers (or frequently only one server) provide software applications to many small client computers.

[11] Business Process Reengineering is managerial jargon for changing how an organisation works by changing procedures, job descriptions and organisational structure to perform a new business function or an existing function differently. However, it may be that BPR is simply another management fad that has often been linked to IS developments. Indeed, it is possible that management and IS journals have left BPR behind and moved on to embrace yet other fads – such as 'knowledge management' (Galliers and Newell 2000). BPR benefits are not altogether uncontested (Davenport 1996). Those of a suspicious mind might even suspect BPR is simply a new(ish) piece of managerial double-speak for job cuts. Indeed, one measurement used for BPR success was simply that headcounts had been reduced by 75 percent (Hammer 1990).

[12] The large degree of physical (as well as cultural) separation between those developing the INCIS software – some of the IBM programmers where not even in the country – compounded this problem of control and agency.

[13] Recommendations of the Inquiry included the following:

1. Business cases should reflect overall technology resources and risks as well as financial issues.
2. Projects should use proven technology. If not, there should be 'increased risk management' processes.
3. Projects need adequate skilled and experience management.
4. There should be separate contracts for infrastructure and applications.
5. Independent quality assurance should be used.
6. Contracts should only be signed when all relevant issues have been resolved.
7. Procedures for Cabinet approval need to be tightened to assure Cabinet receives adequate information and an appreciation of the risks of the project.