VICTORIA

Auditor-General
of Victoria

## SPECIAL REPORT No. 23

# INFORMATION TECHNOLOGY IN THE PUBLIC SECTOR

*Ordered by the Legislative Assembly to be printed*

MELBOURNE
L.V. NORTH, GOVERNMENT PRINTER
1993

No. 26

ISSN 0818-5565
ISBN 0 7306 3461 2


May 1993

The Honourable the Speaker
Legislative Assembly
Parliament House
Melbourne, Vic. 3002

Sir

Under the provisions of section 48A of the *Audit Act* 1958, I transmit the Auditor-General's Special Report No. 23 on Information Technology in the Public Sector.

*Yours faithfully*

C.A. BARAGWANATH
*Auditor-General*

**VICTORIAN AUDITOR-GENERAL'S OFFICE**

**Level 14, 222 Exhibition St, Melbourne Vic. 3000 Telephone: 651 6012 Fax: 651 6050**

# PREVIOUS SPECIAL REPORTS
## OF THE
## AUDITOR - GENERAL

| *Report No.* | *Title* | *Date issued* |
|---|---|---|
| 1 | · Works Contracts Overview - First Report | June 1982 |
| 2 | · Works Contracts Overview - Second Report | June 1983 |
| 3 | · Government Stores Operations<br>· Department Cash Management | October 1984 |
| 4 | · Court Closures in Victoria | November 1986 |
| 5 | · Provision of Housing to Government Employees<br>· Post-Project Appraisal Procedures within the Public Works Department | December 1986 |
| 6 | · Internal Audit in the Victorian Public Sector | December 1986 |
| 7 | · Motor Vehicles | April 1987 |
| 8 | · Foreign Exchange | November 1987 |
| 9 | · Land Utilisation | November 1987 |
| 10 | · Utilisation of Plant and Equipment<br>· Youth Guarantee | November 1988 |
| 11 | · Financial Assistance to Industry | March 1989 |
| 12 | · Alfred Hospital | May 1990 |
| 13 | · State Bank Group - Impact on the financial position of the State | May 1990 |
| 14 | · Accommodation Management | October 1990 |
| 15 | · Met Ticket | November 1990 |
| 16 | · Fire Protection | April 1992 |
| 17 | · Integrated Education for Children with Disabilities | May 1992 |
| 18 | · Bayside Development | May 1992 |
| 19 | · Salinity | March 1993 |
| 20 | · National Tennis Centre Trust<br>· Zoological Board of Victoria | April 1993 |
| 21 | · Visiting Medical Officer Arrangements | April 1993 |
| 22 | · Timber Industry Strategy | May 1993 |

# CONTENTS

# PART 1

# Executive Summary

## 1.1 FOREWORD

In this Report, I have addressed information technology (IT) within the public sector focusing on the illegal use of proprietary software, management controls over software usage and the gross inadequacies in the development of sector-wide human resource management information systems.

The Budget and Economic Review Committee has recently approved a co-ordinated approach to the outsourcing of IT services, with the exception of policy setting, for all Victorian public sector agencies. The aim of the approach is to maximise the outsourcing of IT service provision, consistent with the objective of efficient and effective IT.

The findings in this Report indicate that there has been a failure of government agencies in the past to address fundamental IT controls which has exposed the Government to a number of risks such as excessive costs, ineffective systems and penalties under the *Copyright Act* 1968.

As the Government moves to contract out IT services, it will be even more important to ensure that adequate IT standards are promulgated by the Government to ensure that private sector providers do not repeat the mistakes outlined in this Report. Hopefully, this Report will provide a catalyst for improved management of IT in the future.

## 1.2 SUMMARY OF MAJOR AUDIT FINDINGS

### ILLEGAL AND UNAUTHORISED USE OF SOFTWARE

Page 9

- Sound software control practices were either ineffective or non-existent in most of the agencies reviewed. Formalised procedures for the detection and removal of illegal software had not been developed.

  *Paras 2.24 to 2.25*

- Software and hardware registers were either non-existent or inadequate in most agencies resulting in their inability to identify the existence and location of software.

  *Paras 2.27 to 2.28*

- Only one of the agencies subject to audit review had successfully completed a software audit to determine whether illegal and unauthorised copies of software existed.

  *Paras 2.30 to 2.31*

- Licences or proof of ownership could not be produced by the agencies reviewed for approximately 25 per cent of software loaded onto microcomputers. As a result, exposure to penalties for breach of copyright is significant.

  *Paras 2.35 to 2.37*

- The agencies reviewed are commended for taking immediate action to remove all unlicensed copies of software and put in place policies and procedures to minimise future risk of recurrence. Similar action is now required by all public sector agencies.

  *Paras 2.38 to 2.39*

- Thirty-four per cent of the software in the agencies reviewed had not been authorised by management, the majority of which was not related to the business activities of the agencies.

  *Paras 2.40 to 2.42*

- Shortcomings existed in the procedures used to prevent, detect and eliminate computer viruses.

  *Paras 2.48 to 2.50*

**REVIEW OF THE DEVELOPMENT AND IMPLEMENTATION OF PERSPAY** **Page 23**

- The system development life cycle methodology used to develop PERSPAY was ineffectively implemented.

  *Paras 3.18 to 3.19*

- There are now many payroll applications across the public service, with only 2 agencies actually interfacing with the personnel modules of PERSPAY which is in direct contrast to the initial objective of having a common personnel/payroll system across the public service.

  *Para. 3.28*

- Although delivery of the total system was projected for completion by 1988, development of the payroll module was abandoned in that year and only the personnel functions were finally delivered during 1990.

  *Paras. 3.39 to 3.42*

- The failure to produce the human resource management system within the established time frame has meant that the anticipated benefits of the system did not become available to the agencies. This has resulted in agencies incurring additional expenditure implementing viable interim or replacement systems.

  *Paras 3.29 to 3.30*

- Central agencies failed to sign a contract before the commencement of work by the supplier, exposing the Government to a lack of adequate protection against non-performance.

  *Paras. 3.31 to 3.38*

- A major contributing factor in PERSPAY's inability to meet user needs was the central agencies' failure to either properly translate or include identified user requirements in detailed system specifications.

  *Paras 3.45 to 3.47*

- Detailed costing records were not maintained by central agencies and as a result the total cost of the PERSPAY project cannot be determined.

  *Paras 3.48 to 3.50*

- To date, cost savings of $23.2 million, which were anticipated from the implementation of PERSPAY, have not been achieved.

  *Paras. 3.51 to 3.52*

# PART 2

# Illegal and Unauthorised Use of Software

## Overall conclusion

**2.1** Since the introduction of microcomputers in the early 1980s, their use by government agencies has expanded enormously. However, the ease with which microcomputer software can now be obtained and copied brings significant business risk to agencies due to the potential for illegal and unauthorised software to be used within these agencies.

**2.2** To minimise this risk, it is essential that all government agencies have in place appropriate policies and procedures, including the regular conduct of software audits, to control the use of all software used on microcomputers. The audit review disclosed that most agencies had not developed appropriate policies and procedures to control software use and to identify the quantity and location of software. As a result, the agencies were not only exposed to considerable business risks but also to security and financial risks.

**2.3** Based on the number of illegal copies of proprietary software detected by audit within the agencies reviewed, the Government has a large financial exposure from potential prosecutions under the *Copyright Act* 1968. The audit also found that 34 per cent of software in use was not authorised by management and a significant proportion was unrelated to the business activities of the agencies concerned.

**2.4** The absence of adequate protection against computer viruses left most of the agencies reviewed at risk of data corruption and disruption to their business operations. The detection of viruses in 2 agencies during the review clearly demonstrates these inadequacies.

**2.5** While the agencies reviewed were unaware of the existence of illegal software, it is pleasing to find that they have acted swiftly to remove the software from use. In addition, policies and procedures that address the controls over illegal and unauthorised software and computer viruses have been established.

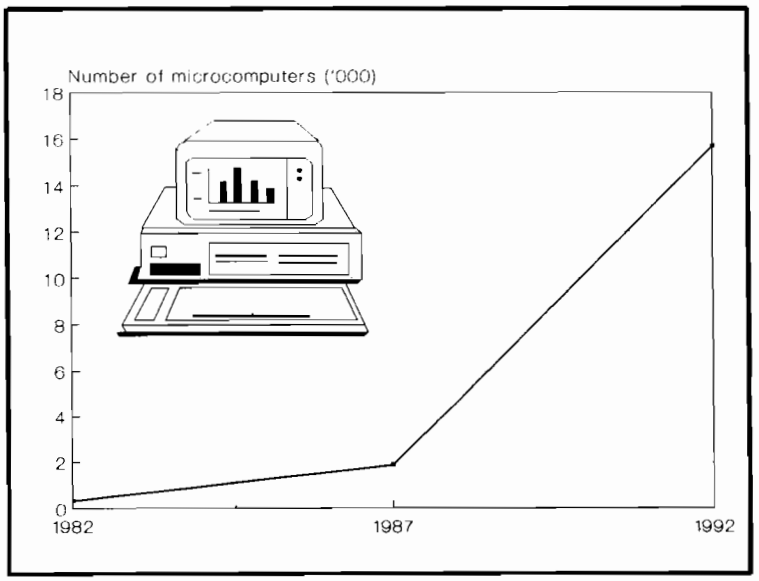
**2.6** It is hoped that this Report will prompt all public sector agencies to review and address the substantial risks that the use of illegal and unauthorised software poses to microcomputers used for business operations.

## BACKGROUND

### Microcomputers in the public sector

**2.7** The use of microcomputers has increased considerably since the early 1980s. Audit estimates that there are in excess of 100 000 microcomputers in use across the public sector. These include 16 000 in budget sector agencies, 26 000 in statutory authorities, 30 000 in colleges and universities and 31 000 in primary and secondary schools. Chart 2A illustrates the increase in the number of microcomputers in budget sector agencies since 1982. This increase is representative of the growth across the public sector.

**CHART 2A**
**GROWTH IN MICROCOMPUTERS WITHIN THE BUDGET SECTOR AGENCIES**




*Source:* Audit survey of government budget sector agencies.

**2.8** Microcomputers are used by almost all agencies to support both their administrative and service delivery functions. In addition, there has been a strong move towards linking microcomputers via local area networks.

### Illegal software

**2.9** Illegal software is defined as the copying and/or use of software without the permission of the copyright owner. The price paid for a legal copy of a software product carries with it the implicit permission for the use of one copy only. In most cases, permission and conditions of use are expressly set out in the form of a licence agreement.

**2.10** According to surveys conducted by the Business Software Association of Australia Ltd (BSAA), at least 50 per cent of all business software products in use in Australia have been obtained illegally. The most common methods of acquisition identified by the BSAA are:

- unauthorised copying of existing software products;
- importation or local production and sale of pirated versions of legitimate software by importers and retailers; and
- importing of proprietary software which under certain licensing conditions is contrary to the provisions of the Commonwealth *Copyright Act* 1968.

**2.11** The factors that contribute to the use of illegal software include:

- user needs not being met by existing software;
- user preference for products not supplied by the employer;
- the ease with which software can be copied; and
- the lack of awareness that copying software is illegal.

**2.12** Apart from the above factors, tight financial constraints and rigid purchase procedures within the public sector can result in users resorting to other methods of obtaining software for operating purposes.

### Unauthorised software

**2.13** Unauthorised software includes any program or application installed without the express approval of the management of that agency. Unauthorised software is installed by users for similar reasons to those contributing to the use of illegal software. The use of unauthorised software creates problems ranging from information incompatibility and destruction of corporate data, through to breaches of security and, potentially, fraudulent misuse of both information and equipment.

### Computer viruses

**2.14** Computer viruses are programs that replicate themselves on computer systems to either deliberately cause nuisance to the owners by displaying messages on the screen or malicious damage through the destruction of computer files. According to the Australian Computer Abuse Research Bureau (ACARB), computer viruses are the fastest growing form of computer abuse in the community.

### Copyright legislation

**2.15** The Commonwealth *Copyright Act* 1968 provides strong legal protection for the proprietary rights of developers and licensed distributors of software.

**2.16** The magnitude of the financial risk involved with using illegal software can be illustrated by the penalties specified in the Act. While it will always remain the prerogative of the courts to determine the extent of penalties imposed for breaches of the Act, the upper limits are as follows:

- The individual liability of both users and management for a first time offence may be as high as $500 for each illegal copy, with a maximum fine of $50 000. Subsequent offences may attract a sentence of up to 6 months jail in addition to the fine; and
- The corporate liability for a first time offence may be as high as $2 500 for each copy with a maximum penalty of $250 000. The fine may increase to $5 000 for each copy in subsequent convictions.

**2.17** In addition to the substantial fines under the Act, organisations and individuals may also face claims for civil damages brought by copyright owners.

**2.18** Government agencies have been targeted for review by bodies, such as the BSAA, seeking to recover damages for illegal use of software. In most cases settlements have been made out of court.

## AUDIT OBJECTIVES AND SCOPE

**2.19** The overall objective of the audit was to ascertain the extent to which illegal and unauthorised software existed on microcomputers within the public sector and to determine whether existing policies and procedures were effective in the detection and prevention of its use.

**2.20** Specific objectives of the audit were to determine whether:

- policies and procedures were in place to control and monitor the use of software on microcomputers and local area networks;
- licences or other proof of ownership could be produced for specific software installed on microcomputers and local area networks; and
- virus protection policies and procedures were adequate to prevent the introduction of computer viruses.

**2.21** Audit examined software resident on microcomputers, local area networks and on floppy disks in 6 agencies, which were considered to be representative of all public sector agencies, and attempted to match the software with licences or other proof of ownership. This process involved running specifically designed audit software programs on selected microcomputers to identify all of the software items installed on each computer. In addition, certain information was sought from a further 100 agencies.

## CONTROLS OVER THE USE OF MICROCOMPUTER SOFTWARE

**2.22** Government agencies should have appropriate policies and procedures which address controls over the acquisition, use and disposal of microcomputer software. Among other things, these controls should provide a basis for detecting and preventing software misuse. Audit is of the view that the policies and procedures, together with the maintenance of appropriate asset registers, and the regular conduct of software audits, provide management with a sound foundation for controlling software use.

### Policies and procedures

**2.23** Policies and procedures covering illegal and unauthorised software, as well as the prevention of computer viruses, should include:

*Illegal software*

- A definition of what constitutes illegal use of software.
- Action to be taken against staff found using illegal software.
- The identification of responsibility for regular software audits.
- Provision for detection and elimination of illegal software through regular software audits.
- Guidance on the disposal of microcomputing software.
- Provision for communication of the policy and regular reinforcement of procedures to all staff.

*Unauthorised software*

- Identification of standard microcomputer products to be used by the agency.
- Evaluation of non-standard products prior to acquisition.
- Provision for detection and elimination of unauthorised software through regular software audits.
- The conditions under which the use of utilities is permitted.
- The use of public domain software, shareware and non-business software.

*Viruses*

- Scanning of all floppy disks prior to use.
- Use of virus detection software on all microcomputers and local area networks.
- Recovery from virus infection in a timely manner.

**2.24** Comprehensive policies covering illegal and unauthorised software and computer viruses were incomplete or non-existent in 4 of the 6 agencies reviewed.

**2.25 The failure to establish comprehensive computer software policies exposes agencies to a number of significant risks, including;**

- **use of illegal and unauthorised software;**
- **introduction of unstable or unpredictable software; and**
- **increased incidence of computer virus infection.**

### Asset registers

**2.26** Software registers, when considered in conjunction with hardware registers, are an effective means of controlling the use of software by enabling an organisation to identify:

- the software it is licensed to use;
- the location of software manuals and both original and back-up copies of software; and
- the computers on which legal software is installed.

**2.27** Audit found that 4 of the agencies reviewed did not have software registers. In addition, while hardware registers existed in 5 agencies, the registers in 3 of these agencies were unreliable.

**2.28 The risks to government agencies of failing to maintain effective hardware and software registers include:**

- **an inability to control microcomputing assets;**
- **difficulty in detecting the existence of illegal and unauthorised software, thereby exposing government agencies to both litigation under the Copyright Act and civil damages; and**
- **an inability to verify the legality of software installed on specific computers.**

### Software audits

**2.29** The most effective method of detecting the existence of illegal and unauthorised software is to conduct a software audit. Such an audit involves the comparison of software, resident on all microcomputer systems and floppy disks, with licensing agreements and agency software registers.

**2.30** At the time of the audit review, 50 per cent of the agencies did not have any formalised procedures for the detection or removal of illegal and unauthorised software. Of the agencies that had formal procedures, only one had successfully completed a software audit.

**2.31 Audit is of the view that the introduction of regular software audits, as part of the internal control framework of each agency, would minimise the risk to government created by the existence of illegal and unauthorised software. Any deficiencies identified during these audits need to be appropriately actioned.**

## INCIDENCE OF ILLEGAL AND UNAUTHORISED SOFTWARE

**2.32** As indicated previously, inadequate attention had been given by most of the agencies reviewed to ensuring appropriate internal controls existed over the use of microcomputer software. Accordingly, those agencies can be exposed to the substantial financial and security risks associated with the use of illegal and unauthorised software on microcomputers, local area networks and floppy disks.

### Illegal software

**2.33 The exposure to the above risks was evidenced by the fact that licences or proof of ownership could not be produced for 25 per cent of the software loaded onto the microcomputers examined.**

**2.34** It is common practice for local area networks to contain fewer licences for an application than the maximum number of authorised network users. This practice, which was adopted by most agencies reviewed, is both cost-effective and legal, as long as the access to each application, at any given time, is restricted to the number of users allowed by the licence. However, audit established that 66 per cent of the agencies did not have facilities to restrict the number of concurrent users to the licenced limit. Further, none of the agencies had a reporting mechanism installed in the system to identify the number of concurrent users at any point in time.

**2.35** As previously stated, there are in excess of 100 000 microcomputers in use within the public sector. Given the audit survey established that on average 25 per cent of the software installed on microcomputers was unlicensed, with 2 or more unlicensed items for each computer, **the potential public sector exposure to penalties arising from breaches of copyright is significant.** For example 5 of the 6 agencies reviewed were each exposed to potential penalties of $250 000 had each instance of illegal software been prosecuted to the maximum penalty. Any civil damage claims initiated by the software proprietors would add to the above amounts.

**2.36** While audit is unable to ascertain the likelihood or extent of penalties being imposed on government, the level of exposure serves to reinforce the material risk to the State from the illegal use of software.

**2.37** Audit recognises that there are costs associated with the removal of illegal copies of software, as well as the cost of purchasing replacement software where it may be necessary for the efficient operation of the agency. However, these costs are considered insignificant when compared with the potential penalties arising from prosecution under the Act.

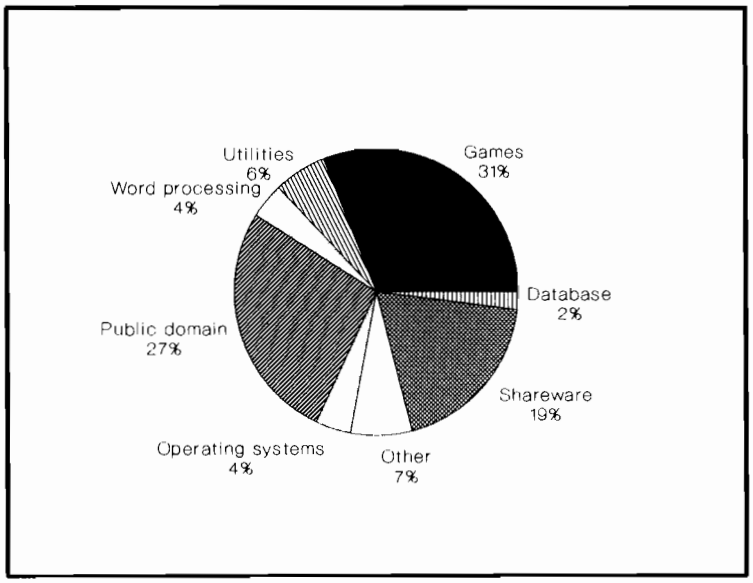
**2.38 The agencies reviewed were alarmed by the audit findings and took immediate action to remove all illegal copies of software. In addition, policies and procedures were put in place to prevent a recurrence in future.**

**2.39 The swift response by these agencies should serve as an example of the action that needs to be taken immediately throughout the public sector.**

## Unauthorised software

**2.40** Audit found that of the microcomputer software used by agencies, 34 per cent had not been authorised by the agencies and a significant proportion of this software, e.g. games, was not related to their business activities. Types of unauthorised software identified during the audit are detailed in Chart 2B.

**CHART 2B**
**UNAUTHORISED SOFTWARE TYPES**




**2.41** The consequences of utilising unauthorised software may include:

- only a limited number of users possessing a working knowledge of the software;
- data which is unable to be transferred or shared as a result of staff using different products;
- the risk of losing information once the user of unauthorised software leaves an agency and the subsequent cost of recovering lost information;
- the need for complex in-house user support for the product, including training and back-up;
- the need for IT support staff to become fluent in more than one of each type of software application diminishes the level of overall service and expertise;
- introduction of unstable or unpredictable software resulting in system breakdowns. As government becomes increasingly dependent on microcomputers, the cost of both down-time and loss of data becomes progressively higher;

- use of specialised software which can by-pass security controls and could potentially be used to change or destroy corporate data; and
- increased susceptibility to viruses and the resultant impact on ongoing activities.

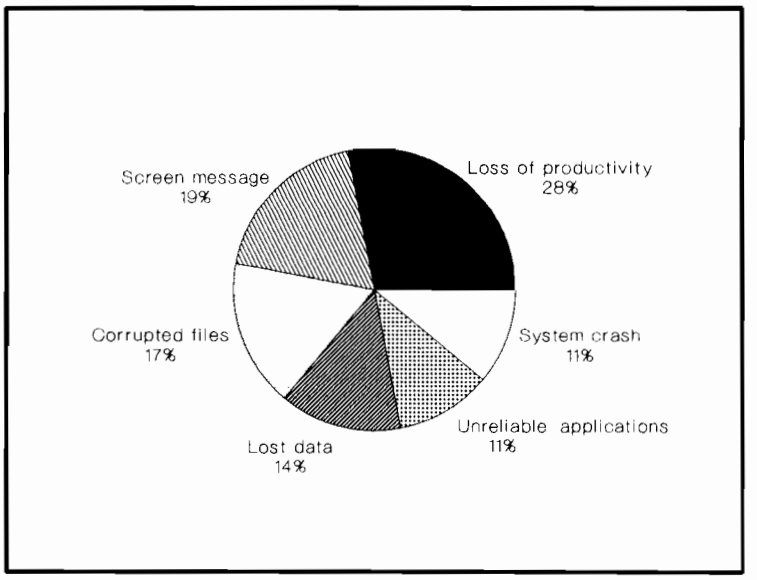
**2.42 Given the risks to the public sector arising from the use of illegal and unauthorised software, agencies need to develop and enforce policies addressing the purchase and use of all software utilised on microcomputers. Such action should be supplemented by regular software audits.**

## RISK OF COMPUTER VIRUS INFECTION IN GOVERNMENT AGENCIES

**2.43** As stated earlier in this Report, the lack of control over the existence of unauthorised and illegal copies of software creates an avenue for the introduction of computer viruses. In assessing the overall risk of viruses to agencies, audit examined the controls in place to prevent, detect and eliminate computer viruses.

**2.44** The consequences of problems caused by computer viruses range from producing unexpected messages on the screen to destroying critical production data. Chart 2C depicts the range of problems caused by viruses.

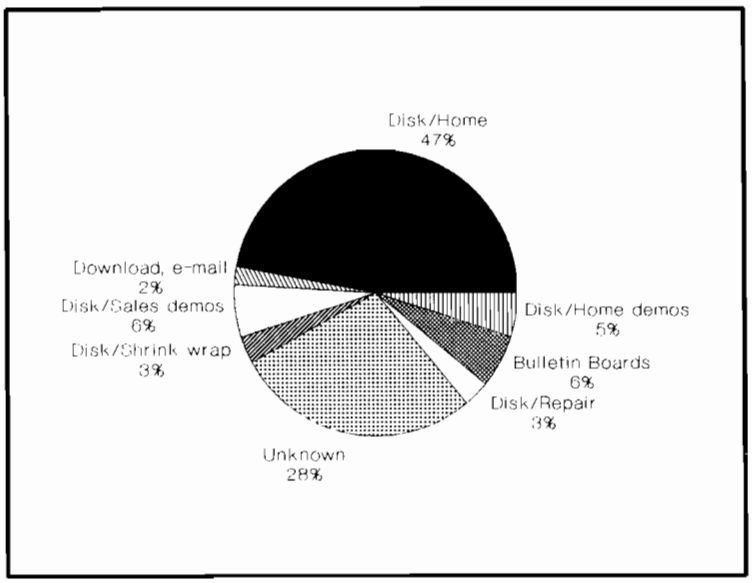
**CHART 2C**
**VIRUS-RELATED PROBLEMS**




*Source:* Computer World, 8 May 1992.

**2.45** Computer viruses can enter an organisation's computer systems by several means. Chart 2D shows the most common sources. The ease with which viruses can enter a system through normal user activity reinforces the fact that strong security measures are crucial to prevent their entry.

**CHART 2D**
**ENTRY POINTS FOR COMPUTER VIRUS**




*Source:* Computer World, 8 May 1992.

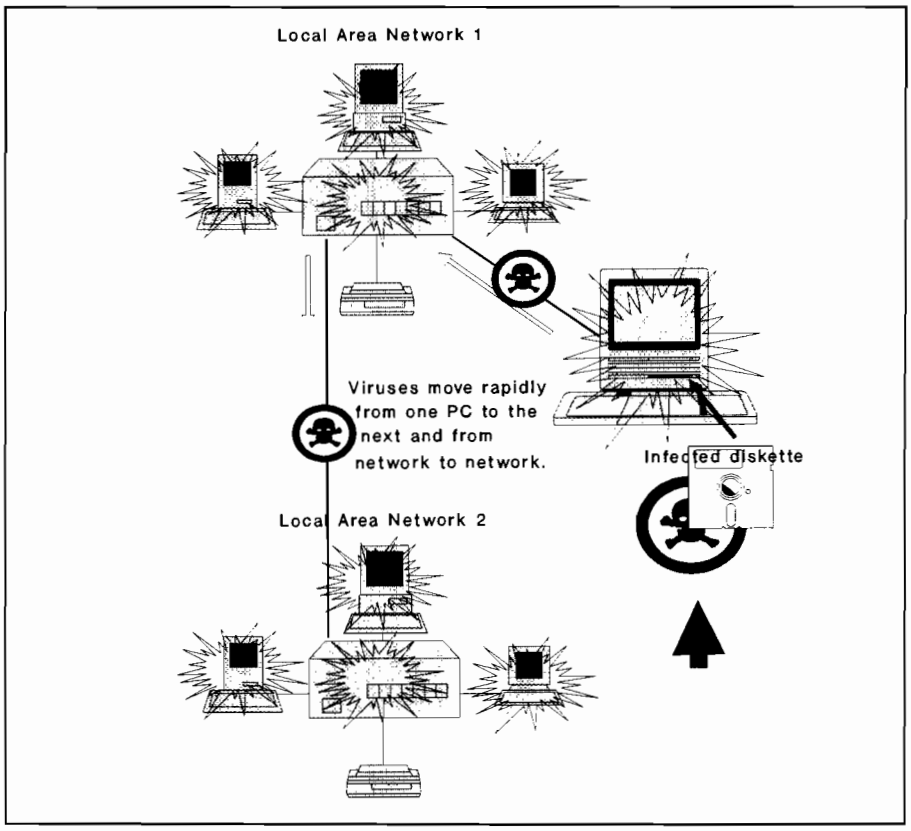
## Incidence of computer virus infections

**2.46** Agencies may incur significant costs as a result of computer virus infection including:

- lost production;
- time required to test all computers and floppy disks;
- time taken to recover any lost data; and
- time involved in attempting to identify the source of the infection.

**2.47** In extreme situations, an agency's computer network could be rendered inoperative by virus infection, particularly as some viruses can spread through networks very quickly as depicted in Chart 2E.

**CHART 2E**
**VIRUS MOVEMENT THROUGH NETWORKS**




**2.48** A number of shortcomings existed, in all agencies reviewed, in the procedures used to prevent, detect and eliminate viruses, including:

- limited use of virus detection software;
- failure to establish *"quarantine stations"* whereby staff are obliged to test floppy disks before use on microcomputers or local area networks; and
- a lack of formal policies concerning the scanning of floppy disks.

**2.49** Viruses were detected in 2 of the 6 agencies reviewed. This illustrates that viruses can enter a system where controls are inadequate. Both agencies involved were notified and the viruses were removed from the systems. The impact of the viruses on those agencies was not determined as it was outside the scope of the review.

**2.50 In view of the inadequacies in protecting computer systems against viruses, there is a need for all government agencies to address this exposure by:**

- **utilisation of up-to-date virus detection software in scanning floppy disks before they are used on microcomputers;**
- **introduction and continual update of active virus detection and removal software on microcomputers and local area networks; and**
- **development of procedures to be followed in the event of a virus infection.**

# PART 3

# Review of the Development and Implemenation of PERSPAY

## Overall conclusion

**3.1** In 1981, government identified the need for a comprehensive human resource management information system for budget sector agencies. In an attempt to meet these needs the design of PERSPAY, as an integrated personnel/payroll system, commenced in 1983. Some 12 years after its conception, the position is as follows:

- the development of the system is still incomplete;
- the needs of users remain unsatisfied; and
- the projected cost savings up to the end of 1992 to the participating agencies of $23.2 million have not been achieved.

**3.2** In addition, further costs have been incurred by agencies in implementing alternative payroll and personnel systems.

**3.3** In audit opinion, the significant factors which have contributed to the failure of PERSPAY include:

- indecisiveness and lack of direction by executive management, particularly central agencies, in monitoring and controlling the project;
- lack of accountability for the development and implementation of PERSPAY;
- the failure of central agencies to enter into a formal contract until 6 years after the supplier commenced development of the system;
- the ineffective implementation of a sound system development methodology to facilitate the efficient and effective development of the proposed system within a specified time frame; and
- deficiencies in the skills of staff involved in the project.

**3.4** The failure of government to successfully develop and implement an integrated personnel/payroll system after 12 years of effort and considerable public expense illustrates the need for adherence to a sound system development methodology. In addition, it highlights the importance of establishing an effective accountability framework and for senior management to actively participate in the development of major IT systems.

## BACKGROUND

### Need for system

**3.5** In 1981, government acknowledged that the existing payroll, personnel and financial management systems operating within budget sector agencies had limited lives and would need replacing.

**3.6** Eventually in 1984, the central agencies, i.e. the former Department of Management and Budget (DMB) and the former Public Service Board (PSB), determined that the integrated information systems now known as FM80 and PERSPAY were the most suitable options to meet the financial and human resource management needs of the budget sector.

**3.7** FM80 was to provide an integrated financial management package which also enabled an automatic transfer of financial information from agencies to the central system at DMB and facilitated centralised cash management.

**3.8** PERSPAY was to provide the integration of personnel and payroll functions within public sector agencies and interface with a central system to supply the central agencies with the human resource information required to effectively carry out their functions.

**3.9** The proposed personnel/payroll system was initially to be developed by DMB and the PSB, in conjunction with a selected external software supplier. An inter-agency committee, called the Government Resource Management System (GRMS) Committee, was established within DMB in March 1983. A primary function of the Committee was to develop guidelines and standards to address centralised systems across the Victorian public service.

**3.10** The following benefits were envisaged from the development and implementation of PERSPAY:

- more comprehensive and accurate information would be available to agencies on a timely basis;
- facilities would be provided for salary forecasting and modelling; and
- scope for rationalising work practices such as decreasing the staff in personnel and payroll by combining the 2 functions and integrating leave records with payroll information.

## AUDIT OBJECTIVES AND SCOPE

**3.11** The overall objective of the audit was to evaluate the extent to which economy, efficiency and effectiveness was achieved in the development of PERSPAY.

**3.12** Specific objectives of the audit were to determine whether:

- adequate analysis of agency payroll and personnel requirements was conducted;
- user needs were adequately met; and
- the development of the system was achieved within the established scheduled time frame.

**3.13** The scope of the audit focused on management procedures at DMB and the PSB and the examination of systems at selected user agencies.

**3.14** As part of the audit process, documentation was examined and discussions were held with representatives of 10 government departments.

## METHODOLOGY REQUIRED TO DEVELOP INFORMATION SYSTEMS

**3.15** Business entities often commit considerable resources, both in terms of manpower and cash outlays, to the development, acquisition and maintenance of information systems. A successful system becomes a valuable asset and needs to be protected and controlled.

**3.16** The process followed in the development, acquisition and maintenance of information systems should attempt to achieve system effectiveness, economy and efficiency, data integrity, resource safeguarding and compliance with laws and regulations. The use of an effective system development life cycle (SDLC) methodology should provide an organisation with a reasonable assurance that these objectives will be achieved.

**3.17** The SDLC methodology should:

- establish the roles, responsibilities and accountability of the central agencies, user departments and others, for planning, developing, reviewing, implementing and auditing the end product of the system development process;
- be reviewed periodically by the organisation's senior management to ensure that its provisions reflect current, generally accepted, techniques and procedures;
- provide for the creation of a clearly stated written definition of the nature and scope for every system development project before work on the project begins;
- provide for the participation by user departments in the definition and authorisation of an information system development or modification project;

- specify the basis for assigning staff to project teams and defining the responsibilities of the various team members;
- provide that the information needs of users to be satisfied by the existing and the proposed new, or modified, system were clearly defined before a development or modification project was approved; and
- provide for the approval by designated members of management of the work accomplished in each phase of the cycle before work on the next phase begins.

**3.18** A PERSPAY steering committee was established in early 1983 which considered the use of a commercial system development life cycle methodology package known as SDM70. However, the steering committee was of the view that the methodology was unlikely to be appropriate for PERSPAY and that its development could be better catered for by an internally developed option based on the principles of SDM70. The methodology adopted outlined that the project would proceed over 5 major phases, namely:

- requirements specification;
- design alternatives;
- development;
- testing; and
- implementation.

**3.19 Audit is of the opinion that while the methodology adopted included most of the key aspects required in a SDLC, its overall implementation was ineffective. In particular, the requirements specification and design phases set targets which proved to be unobtainable. Failure of an organisation to effectively utilise a SDLC methodology can seriously jeopardise the success of a system and result in significant wastage of financial resources.**

- *RESPONSE provided by Secretary, Department of Finance*

  *The systems methodology adopted by DMB (as agreed by the Steering Committee) was based on the principles of SDM70. This approach, although it did not follow the formal application of SDM70, utilised prototyping, joint applications development and structured data modelling which was considered more suitable for the development of the proposed software.*

**3.20** The impact of the ineffective implementation of a sound SDLC methodology in the development of PERSPAY is outlined in the following pages of this Report.

## Development of PERSPAY

**3.21** After the need for a computerised human resource management (HRM) system was identified in 1981, minimal time was devoted to the development of PERSPAY, with a higher priority afforded to the development of FM80 over the following 2 years. A protracted period, from 1983 to 1986, was devoted to the establishment of various committees and development of preliminary planning documents and specific system requirements.

**3.22** In 1986, following the calling of tenders for the PERSPAY project, a supplier was selected and a phased development approach was adopted by the central agencies.

**3.23** At that stage, it was projected that the project would be completed within 2 years. Releases 1 and 2 of PERSPAY, which met most of the personnel module requirements, were delivered during this period. However, the supplier failed in its attempt to develop the payroll component.

**3.24** A change in direction by the central agencies in late 1988 was brought about as a result of the supplier failing to develop the payroll module and incurring substantial cost overruns. For the next 9 months, the supplier attempted to develop an interface between 2 payroll systems it had previously developed and the personnel module of PERSPAY. However, this exercise also failed resulting in user agencies being advised by the central agencies to choose their own payroll bureau solutions. This decision was viewed by audit and agencies expecting to utilise the system as a virtual admission by government of the failure of PERSPAY to achieve one of its major objectives, namely of providing a common payroll system across the public service.

**3.25** As an alternative, arrangements were to be undertaken by user agencies to interface a payroll bureau system with the personnel, establishment and leave modules of PERSPAY which had been developed. However, agencies were free to implement any payroll system which met the specified standards but were required to show to the GRMS Committee justification on functionality.

**3.26** The supplier suspended further development of system interfaces in May 1990 after expressing concerns that the consideration of more than one payroll solution would create 2 problems.

**3.27** Firstly, the agencies would not have a uniform system, which was contradictory to government's original direction chosen with PERSPAY. Secondly, as the supplier was to be engaged as only one of a number of software suppliers to government agencies, its returns from such activities were considered too small to risk the continued cost of developing and supporting a payroll module for PERSPAY which was unlikely to ever succeed.

**3.28** During 1990, agencies formed the view that central management was taking a back seat role in the issue of developing the payroll module after being obliged to seek suitable payroll alternatives. There are now multiple payroll solutions across the public service, with only 2 agencies actually interfacing with the personnel modules of PERSPAY. This is in direct contrast to the perceived benefit of having a common payroll system across the public service to reduce development and training costs and resource requirements. It also means that the 1981 vision of a government-wide integrated personnel/payroll system has been forgone.

**3.29 PERSPAY's failure to satisfy public service requirements has resulted in agencies being forced to develop separate human resource management systems requiring further use of valuable time, personnel and money, in addition to the considerable cost and use of resources already expended by the Government on PERSPAY development.**

**3.30 In summary, some 12 years after the idea of an integrated personnel and payroll system was envisaged, apart from certain personnel modules being provided, a product suited to the needs of the Victorian public service has not been delivered.**

- *RESPONSE provided by Secretary, Department of Finance*

  *It is acknowledged that the PERSPAY project was not completed within the original time frame nor the original objective achieved. However, the 12 year time frame specified does not accurately represent the life span of the revised PERSPAY project. The project effectively commenced in 1984 with the period between 1981 to 1984 involving investigation of existing systems and general planning on new systems for the budget sector. Due to resource constraints, the Financial Management System project had priority and commenced before PERSPAY. The administration of the PERSPAY system was handed over to the Public Service Board on 1 July 1990, the Central Database was signed off by the PSB in April 1991 and the contract was signed by the Minister for Finance in December 1992.*

  *The audit report does not acknowledge the decision made in 1988 not to proceed with the payroll component of PERSPAY due to the supplier's inability to meet the cost of development within the original price quoted. Further, the payroll interface did not proceed as a result of a change in ownership by the vendor in 1989. Recognition has not been given to the availability of interfaces between PERSPAY and 2 payroll products, Newpay and HRINSIGHT.*

  *The central agency role was to make a system available to agencies with agencies responsible for justifying investment decisions for acquisition of software/hardware and implementation of systems. In addition, government IT policies at that time allowed departments to "implement resource management systems in a way that best fits their environment". Consistent with this philosophy, Government Resource Management Systems Standards were developed by DMB to assist agencies with the above approach. DMB did not deter agencies from introducing systems other than FM80 or PERSPAY if the standards were met and necessary approvals obtained.*

  *Although implementation was essentially a departmental issue, a basic implementation package and related documentation was negotiated with the PERSPAY supplier.*

## Contract negotiations

**3.31** A draft contract and software support agreement with the chosen supplier was developed but not signed prior to the supplier commencing in 1986. Audit was unable to ascertain the specific reasons for the failure of the central agencies to reach agreement and subsequently sign a formal contract. However, in audit opinion, one of the key factors was the failing of central government agencies to control and drive the negotiation process with the software supplier.

**3.32** The ownership of the supplier firm changed a number of times from 1988 to 1989, with each new owner assuming the responsibilities associated with the development of PERSPAY. Each transfer of ownership brought with it a different outlook on the proposed terms and conditions of the contractual arrangements, consequently complicating and protracting the contract negotiations.

**3.33** The failure to originally sign a contract in 1986 identifying project deliverables, the scheduled time frames in which they were required and appropriate penalty clauses, led to a lack of adequate protection for government against the non-performance of the supplier and a possible loss of incentive for the supplier to use best endeavours to meet government's requirements.

**3.34** In recognising the failure of the supplier after 6 years to successfully develop an integrated personnel and payroll system, DMB in early 1991 sought to take legal action against the supplier. To this end, DMB received advice from a firm of solicitors which in part stated: *"You are entitled to specific performance of the agreement, even though the contractor states that it is uneconomic for it to perform the terms of the agreement. If the contractor refuses to proceed, you may apply to a court for an order for specific performance of the agreement and/or damages. Examination of the financial status of the contractor would be highly desirable before deciding whether or not to institute proceedings. Your instructions and our advice could not be much more than superficial, given the time constraint"*. DMB decided not to pursue legal action.

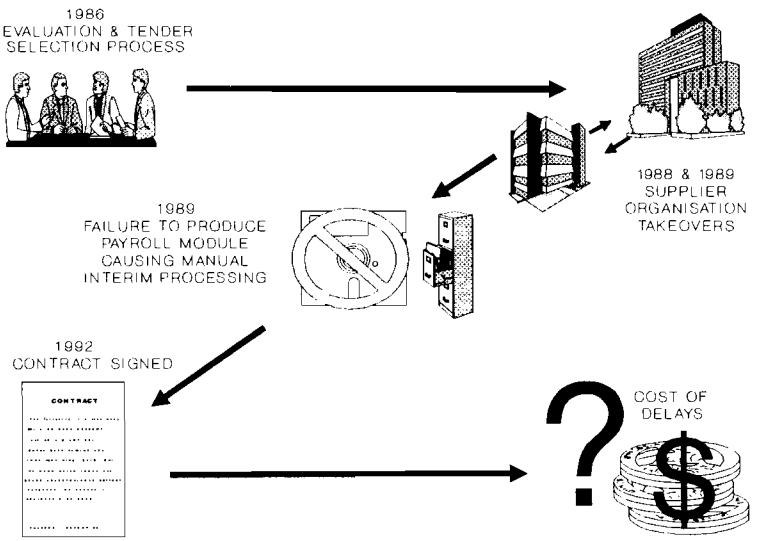
**3.35** A contract between the Minister for Finance and the supplier was finally signed on 16 December 1992. Audit ascertained that the Department considered it was important to have a contract signed for the following reasons:

- to gain access to the source code in a contingency situation;
- as recognition of ownership of PERSPAY by the Government; and
- the absence of a contract would leave the PERSPAY system vulnerable in the case of either an emergency or failure to deliver an effective, economical service by the supplier.

**3.36 While signing the contract formalises the protracted process to date, audit is of the view that such action only serves to relieve the supplier of any liability for past failure to meet the specified requirements under the Heads of Agreement. The contract no longer reflects the original scope of the project.**

**3.37** The outline of the contract time frame is shown in Chart 3A.

**CHART 3A**
**OUTLINE OF CONTRACT TIME FRAME**




**3.38 For the protection of scarce government resources, there is a need to ensure that enforceable written contracts are entered into prior to the commencement of future major IT projects.**

- *RESPONSE provided by Secretary, Department of Finance*

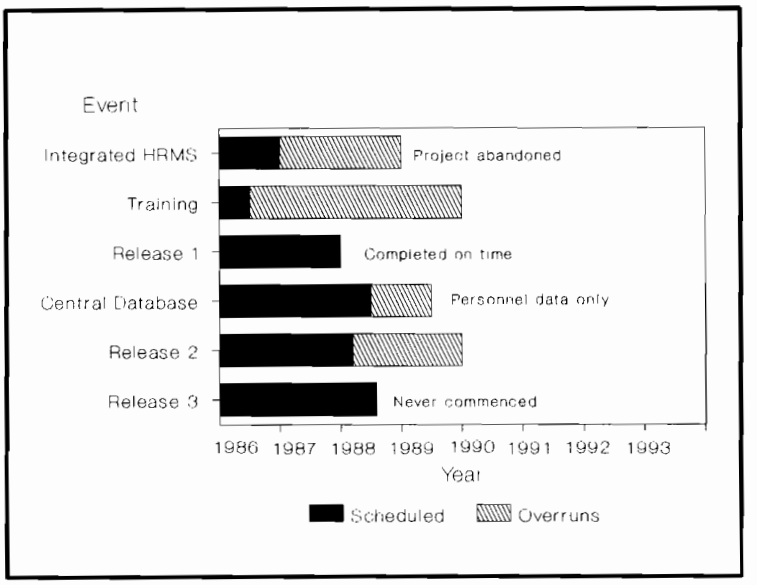
  *The need to have adequate contract documentation signed prior to the commencement of work by external service organisations is acknowledged. Delays in signing the contract were impacted by the 2 changes in ownership of the software supplier. The contract, as formalised, reflects the decisions made in 1988 to 1990 not to proceed with the payroll component or payroll interface.*

## Failure of supplier to meet time constraints

**3.39** Delivery of the total system was projected for completion by 1988, however, the development of a payroll system, which included an automatic interface to the personnel system, was abandoned in that year. The personnel system was eventually developed and implemented in 1990.

**3.40** Chart 3B illustrates a comparison of scheduled and actual completion dates for various components of the PERSPAY project.

**CHART 3B**
**PERSPAY PROJECT SCHEDULE**




**3.41** The reasons for the lengthy delays in the development process for PERSPAY were many and varied, but the key factors were:

- poor planning and scheduling procedures in the initial stages of the project;
- inability of the supplier to develop the payroll module;
- the subsequent financial instability and uncertainty of the ongoing operation of the supplier diminished confidence in the firm's ability to complete the development process;
- a lack of ongoing support of PERSPAY by the supplier; and
- technical difficulties encountered in installing software programs, which reduced the product's functionality.

**3.42 Overall, audit considered that the project management was inadequate and there was a serious lack of direction, monitoring and accountability from executive management. These deficiencies were further exacerbated by a high turnover of project staff, including several changes in the project leader, due in part to the length of the development and implementation processes.**

- *RESPONSE provided by Secretary, Department of Finance*

  *The DMB approach to the acquisition of a personnel-payroll system in the mid-1980s was forward looking. When PERSPAY was conceptualised and a tender issued, there were a limited number of integrated human resource management (HRM) systems available compared with current technologies. Fully integrated packages did not appear in the market until about mid-1989 and there is now a variety of HRM packages available today that were not available in the mid-1980s.*

*In recognition of the need to supplement project management skills within DMB as well as providing technical and HRM expertise, an accounting firm was employed from January 1986 to April 1989 for specific tasks as well as to assist, advise and participate in the PERSPAY project. Over that time, the consultants also acted as project manager over a limited period.*

## Failure of PERSPAY personnel module to meet user needs

**3.43** Although the payroll functions of PERSPAY were never successfully developed, the personnel modules were regarded as completed in 1990. However, the inability to interface those functions with separate payroll systems ultimately reduced the overall effectiveness of the public service human resource management system.

**3.44** Furthermore, the personnel module, which the central agencies consider has been completed, contains the following serious deficiencies:

- the system is not user-friendly;
- manuals do not meet user needs;
- the report writing module is time consuming and unreliable; and
- PERSPAY does not have the capability to process all the employment and personnel information requirements.

**3.45** Audit is of the view that as a result of the above factors PERSPAY currently has a low level of usage and credibility within agencies and fails to provide sound information to assist the management decision-making process. **In audit opinion, a major contributing factor in PERSPAY's inability to meet user needs was the central agencies' failure to either properly translate or include identified user requirements in the detailed system specifications.**

**3.46** The few agencies that managed to operate PERSPAY with any degree of success required additional full-time human resource management staff with a relatively high level of computer proficiency to maintain the system.

**3.47 It is important that management and user groups have active involvement in documenting and designing systems to prevent expending resources on systems that will not satisfy their business requirements. Without user support and management commitment the benefits of information systems may never be realised.**

- *RESPONSE provided by Secretary, Department of Finance*

  *With respect to user requirements, a number of documents were prepared in consultation with a working party of 17 practitioners from agencies, circulated to all agencies for comments, signed-off and also independently reviewed and endorsed by external consultants. The detailed function system specification (DFSS) was developed by an external party with user participation as mentioned and endorsed by an accounting firm. This included the DFSS which was used as the basis for prototyping and joint applications development.*

  *It is expected that a user's perspective and expectations of what is required and achievable will change dramatically over time especially in the availability and sophistication of HRM systems between 1986 to 1989 and 1991-92 when interviews were conducted by audit.*

*Users of PERSPAY are continuing to add further modules to enhance the core PERSPAY product. For example, further modules were acquired in 1991 and in 1992, the system was enhanced to accommodate the recent Office Based Structure requirements. It is expected that user requirements will change over time and any product will need to be enhanced to meet emerging user demands.*

## COST OF DEVELOPING PERSPAY

**3.48** Detailed budgets are normally prepared at the commencement of any project and are based on requirements identified and tenders submitted. It is crucial for management to monitor, on an ongoing basis, actual against budgeted costs and ensure cost overruns are promptly identified and minimised. If this monitoring process is neglected, the use of budgets as a management tool is diminished.

**3.49 Audit found that data on the total cost of developing the PERSPAY project, including overheads, was not maintained by the central agencies involved. Due to the absence of detailed costing records, the total cost of the project cannot be calculated but would amount to several million dollars, inclusive of overheads and the need for agencies to eventually implement alternative systems to PERSPAY.**

**3.50** The failure to develop mechanisms to progressively monitor costs also inhibited the ability of management to effectively measure whether the expenditure justified the projected benefits.

**3.51** The major benefit from the PERSPAY project, according to DMB, was to have been the projected level of cost savings. Based largely on anticipated reductions in staff arising from the redeployment of human resources in personnel and payroll functions, DMB estimated the potential cost savings over the 5 years to 1990-91 were $14.3 million. On the basis of DMB assumptions, audit has extended this calculation to include anticipated savings for all years up to the end of 1992 as illustrated in Table 3C.

**TABLE 3C**
**PROJECTED SAVINGS**
($'000)

| | *Steering Committee estimation* | | | | | *Audit estimation* | | |
|---|---|---|---|---|---|---|---|---|
| *Saving categories* | *1987-88* | *1988-89* | *1989-90* | *1990-91* | *Total* | *1991-92* | *Dec '92* | *Total* |
| Systems replacement - | | | | | | | | |
| PERSYST | 110 | 110 | 110 | 110 | 440 | - | - | 440 |
| PAYCOST | 100 | 200 | 250 | 250 | 800 | - | - | 800 |
| Staff redeployment | 1 060 | 2 735 | 3 980 | 5 155 | 12 930 | 5 875 | 2 937 | 21 742 |
| Other hardware savings | 40 | 40 | 40 | 40 | 160 | 40 | 20 | 220 |
| **Total savings** | **1 310** | **3 085** | **4 380** | **5 555** | **14 330** | **5 915** | **2 957** | **23 202** |

**3.52 Audit estimated that anticipated cost savings of $23.2 million would have been available to government agencies up to the end of 1992. These savings have not been achieved. The level of economy and efficiency achieved during the development of PERSPAY cannot be measured due to the absence of detailed costing information. In addition, the central agencies failed to undertake a post-implementation review of the effectiveness of the personnel module introduced in 1990.**

- *RESPONSE provided by Secretary, Department of Finance*

  *Funding provided for the project was within overall budgeted estimates and properly recorded and reconciled. No additional funding was sought by the Department for the development or enhancement of PERSPAY. Annual maintenance expenditure has been incurred by users consistent with externally maintained software.*

  *Recognition has not been given to the savings accruing from and improved personnel information available, following the introduction of computerisation of previously manual personnel systems in agencies. Staff savings were achieved in the Public Service Board following the introduction of the PERSPAY Central Database which utilised automated maintenance and updates, which were not possible with the previous systems, PERSYST.*

## PREVIOUS AUDIT REPORT

**3.53** In the foreword to my *Report on Ministerial Portfolios, May 1993,* I referred to the need to improve resource management in the public sector and the fact that there had been a failure of government agencies to respond positively and effectively to audit representations, particularly those relating to inadequacies in information and controls systems.

**3.54** Many of the deficiencies identified in this Report are similar to those contained in representations made by my Office to DMB in 1987 following an audit which identified problems associated with the development of a computerised financial management system (FM80) for budget sector agencies.

**3.55** While the audit recommendations arising from the 1987 audit were well received by DMB at that time, the current audit findings indicate that there has been a failure to implement the promised remedial action which has resulted in the outcomes detailed in the preceding paragraphs.

## FUTURE DIRECTIONS IN GOVERNMENT INFORMATION SYSTEMS DEVELOPMENT

**3.56** As a matter of urgency, the Government must ascertain the need for both the existence and implementation of either an integrated or interfaced personnel and payroll package across the public service. If the need is affirmed, the Government should evaluate the options, determine the appropriate strategies, assign management responsibility and establish accountability processes for the implementation of the selected option.

**3.57** The failure of government to successfully develop and implement an integrated personnel/payroll system after 12 years of effort and considerable public expense should serve as an example for future administrations of the problems that can arise with a major project where there is a lack of strong direction, poor planning, inadequate budgeting and project administration and a lack of attention to the needs of users. **It is critical that the development of all future information systems implemented by government include:**

- **establishment of a policy framework for the overall direction and central monitoring of major system developments;**
- **development of policies to identify the management responsibilities, accountability framework and monitoring requirements associated with the creation of centralised information systems;**
- **post-implementation reviews to ascertain if the projected benefits of new systems have been realised and to develop solutions that address any inadequacies; and**
- **utilisation of a sound, well-structured and proven SDLC methodology when acquiring, developing or maintaining information systems within the public service.**

■ *RESPONSE provided by Secretary, Department of Finance*

*The issue of future development/acquisition/management of new software systems for application in departments will need to be considered in the overall context of government policies for the management of the budget sector.*

## EMERGING ISSUES

### Outsourcing of IT services

**3.58** The Government, in April 1993, issued a policy statement on outsourcing of IT services which requires all government agencies to maximise outsourcing opportunities subject to cost-efficiency and security considerations. The Government envisages that 70 per cent of all public sector IT services will be outsourced by December 1994.

**3.59** While acknowledging the new policy and the continuing need for in-house expertise in agencies, an audit review prior to the release of the policy identified a number of deficiencies with the use of external IT specialists.

**3.60** The audit review established that inadequate attention has been given by most agencies to the development of human resource plans to identify staffing numbers, skill levels and strategies required to successfully implement IT strategic plans. As a result, staffing shortfalls and a lack of desirable skills impacted upon the development of systems and provision of IT services in the most efficient and effective manner.

**3.61** In particular, difficulty was experienced by agencies in recruiting and retaining specialist IT staff due to differentials between public and private sector remuneration rates. While staffing shortfalls and lack of specialist expertise were often met through the engagement of external specialists on a contractual basis, this action was also seen to have certain disadvantages, including:

- external contractors costing more than in-house staff;
- a gradual erosion of skills of in-house staff which impacted on their ability to manage the activities of contractors in terms of ensuring the most desirable output within specified time frames; and
- increasing reliance by agencies upon certain contractors due to their specialist knowledge of an agency's operations and, as a result, services were not always provided at competitive prices.

**3.62** Audit considers that the implementation of the outsourcing policy increases the need for agencies to address the deficiencies identified in the audit review. In particular, agencies will need to:

- evaluate their corporate goals and determine whether their existing IT strategy is appropriate to the achievement of those goals given the increased business opportunities arising from outsourcing;
- understand the challenges and management implications of IT and to assume effective management control of planning, development of strategies, technical performance and quality control;
- ensure that all external services are delivered with due regard to competition and in the most effective and cost-efficient manner;
- develop IT management frameworks which are conducive to controlling the agencies' relationships with external providers; and
- establish performance indicators whereby the quality and efficient delivery of external services can be measured in relation to meeting an agency's objectives.

# Appendix A

# Glossary of terms

## GLOSSARY OF COMPUTER TERMS

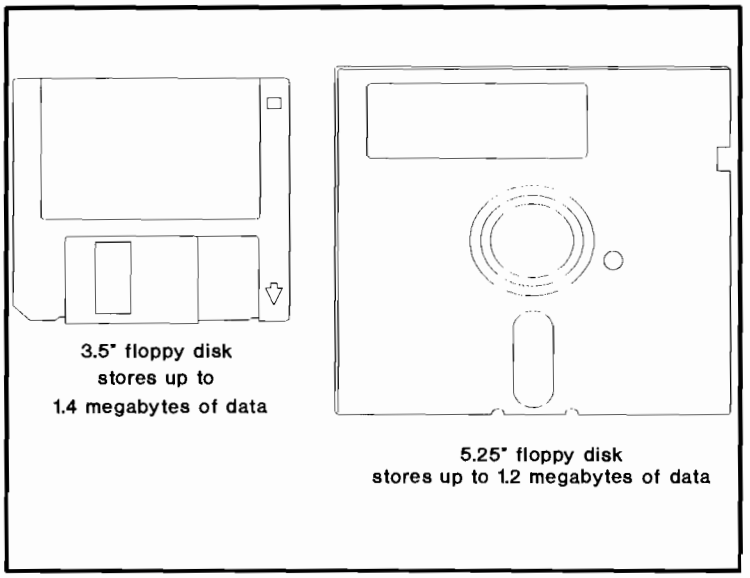
*Application* — A collection of programs and procedures which provide a functional computer solution to a problem.

*Concurrent users* — The number of users on a network accessing an application or facility at any given time.

*Directory* — A table of contents for a disk. The directory contains the names and other relevant information of the files stored on the disk.

*Floppy disk* — A flexible and removable, low-cost storage device capable of storing limited quantities of data.

**CHART A1**
**FLOPPY DISKS**




*Hard disk* — A storage device capable of storing and retrieving large quantities of data rapidly. Hard disks are usually built into the microcomputer.

*Human resource plan* — A human resource plan links resource needs to corporate goals. The plan also identifies resource requirements and the strategies available to facilitate their acquisition in the most effective and economic manner. Resource plans should be particularly detailed and include skill requirements, duration of employment and timing of resource acquisition.

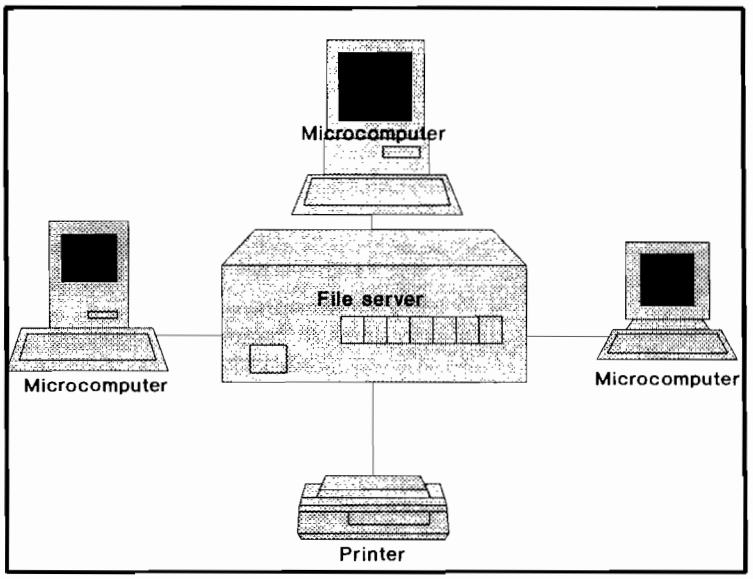
*Information technology strategic plan*

Outline of strategies which, if effectively implemented, will allow agencies to achieve the information technology strategic directions identified in their corporate plan.

*Local area network*

A local area network is a collection of microcomputers connected by special cables, usually to a more powerful microcomputer called a *"file server"*. Local area networks allow data, programs and other resources to be shared by all the microcomputers connected. One of the key features of a network is shared storage for corporate data and programs while retaining personal storage areas, called *"personal directories"*, for user data. In most cases, a local area network administrator manages access to the network resources and provides support to users.

**CHART A2**
**LOCAL AREA NETWORK**




*Microcomputer*

A *"microcomputer"* is the term applied to a computer that may be used by a single individual at any point in time. It is also frequently called a *"personal computer"*. Microcomputers require software, which comprises a series of instructions called *"programs"* to enable the microcomputer to be used.

*Operational plans*

Operational plans translate Strategic Plans into frameworks prepared annually to enable the effective and efficient management of all resources.

| | |
|---|---|
| *Package* | A collection of programs which provide the functionality required to complete all the computerised tasks required in an application. Most microcomputer software packages are purchased off-the-shelf. |
| *Personal directory* | The table of contents for the personal storage area on a local area network reserved for each individual user. |
| *Program* | A series of instructions written in computer language which instruct the computer to perform a task. |
| *Public domain* | Programs that have no copyright and can be used or copied by any person. The authors have placed the programs in the public domain arena for all the public to use. |
| *Shareware* | Programs that are available for use on the principle that if the program suits a user's needs and it is intended to be used regularly, then the user is obliged to send the author a registration fee. |
| *Software* | A single program or a collection of computer programs. |
| *System development life cycle* | Formal procedural document which outlines the many activities which must be performed when developing a system. |
| *Utilities* | Commercial software comes in 3 broad categories: operating systems, applications and utility programs. Utilities are generally designed to complement the operation of other software or to manage the computer environment. Utility programs allow the user to perform specialised routines in addition to those provided by the computer's operating system. |