2007 No. 17

2007

PARLIAMENT OF TASMANIA

AUDITOR-GENERAL
SPECIAL REPORT No. 69

Public building security

October 2007

Presented to both Houses of Parliament in accordance with the provisions of Section 57 of the Financial Management and Audit Act 1990

By Authority:

Government Printer, Tasmania

Auditor-General's reports are available from the Tasmanian Audit Office, HOBART. This report and the recent titles shown at the back of this report can be accessed via the Office's home page. For further information please contact:

Tasmanian Audit Office
GPO Box 851
Hobart
TASMANIA 7001

Phone: (03) 6226 0100, Fax (03) 6226 0199
Email: admin@audit.tas.gov.au
Home Page: http://www.audit.tas.gov.au

This report is printed on recycled paper.

ISBN 0 9775898 7 0

16 October 2007

President
Legislative Council
HOBART

Speaker
House of Assembly
HOBART

Dear Mr President
Dear Mr Speaker

SPECIAL REPORT NO. 69
Public building security

This report has been prepared consequent to examinations conducted under section 44 of the *Financial Management and Audit Act 1990*, for submission to Parliament under the provisions of section 57 of the Act.

The compliance audit was to ascertain whether departments had adequate physical security procedures in place at the operational level to meet their obligations.

Yours sincerely

H M Blake
AUDITOR-GENERAL

This page left blank intentionally

CONTENTS

Foreword

This compliance audit examined security arrangements at government buildings that have a high degree of public access and complements compliance audit *Building security*, Special Report No 60 – tabled May 2006.

Public sector staff and customers have an expectation that they will be able to go about their business in a safe environment where premises, information and assets are secure.

This audit reviewed security arrangements at schools, libraries, *Service* Tasmania shops and hospitals, encompassing three government departments. Effective security procedure and practice can minimise exposure to risk to personal safety and well-being as well as government property and information.

While there are some areas of concern, the standard of security at the premises audited was generally satisfactory. However, incident reporting could be improved and there is a need to ensure that site management apply consistent, effective procedures and solutions to security issues to preserve a safe environment for staff and the public.

Based on the sample of departments audited I also concluded that a systematic risk analysis aimed at identifying security risks and vulnerability was not undertaken, in some cases security policies and procedures were incomplete or needed updating and there was a lack of awareness by staff of existing security policies and procedures.

This led to eighteen recommendations being made aimed at improving security.

HM Blake

Auditor-General

October 2007

List of acronyms and abbreviations

Agencies	Collective term used in this Report to cover Government departments and other Government entities
DIER	Department of Infrastructure, Energy and Resources
DOE	Department of Education
DPAC	Department of Premier and Cabinet
DPIW	Department of Primary Industries and Water
DPEM	Department of Police and Emergency Management
SEO	School Executive Officer
DEM	Department of Emergency Medicine
CCTV	Closed circuit television
Risk management standard	Australian/New Zealand Risk Management Standard AS/NZS 4360:2004

Executive summary

Executive summary

Introduction

In the compliance audit, *Building Security* (Special Report No 60 of May 2006), we reviewed public sector buildings at selected government office buildings. These buildings were not generally accessible to the public. This audit, *Public building security*, focussed on physical security at buildings that have a high degree of public access.

Departmental Secretaries have an ethical and legal responsibility to adopt sound security management practices to protect their customers and staff, ensure privacy of information and safeguard assets. Security of public sector buildings is required to protect staff and property from threats such as:

- unauthorised physical access
- theft of assets and personal property
- assaults on staff and visitors
- wilful damage including arson, graffiti, vandalism and damage from burglary
- misuse of assets, fraud and sabotage.

The object of the audit was to ascertain if buildings that are accessible to the public were subject to sound security management. Risk assessments should be used to identify risks and vulnerability. Policies and guidelines link risk assessments to the implementation of appropriate and cost-effective security measures. Responsibilities for security should be allocated to staff.

Buildings should have a clear delineation between public access areas and secure staff work areas to protect assets and confidential records.

Security incidents that occur should be documented in such a way as to allow effective monitoring and review. Responses to security incidents need to be appropriate and effective.

Findings

We found:

- Not all departments reviewed had undertaken a systematic risk analysis to identify security risks and vulnerability.
- Security policies and procedures were incomplete or needed updating at two of the departments reviewed.
- Lack of awareness by staff of existing security policies and procedures.

- Failure to allocate security responsibilities to appropriate staff.
- Generally, effective security measures were being implemented.
- Security incident record keeping could be improved at two of the reviewed departments.
- Monitoring and review was inconsistent across the three departments audited.

Recommendations

In all, we made 18 recommendations aimed at addressing the findings described above and to enhance security procedures for all government departments.

Principally, these recommendations were targeted at:

- Improving the risk management culture for building security.
- Allocation of security responsibilities.
- Identification of security training needs.
- Improving the quality of policy and procedures.
- Better recording and monitoring of security incidents.

This page left blank intentionally

Recommendations and management response

Recommendations and management response

List of recommendations

The following table reproduces the recommendations contained in the body of this report.

No	Report Section	Page	Recommendation
1	1.2 2.2 3.2	17 24 36	We recommend that a comprehensive security risk analysis that is regularly reviewed and updated be implemented at all public access sites.
2	1.3.1 2.3.1	18 25	We recommend details of security policies and guidelines be effectively communicated to staff and appropriate procedures be kept up-to-date and tested regularly.
3	1.3.2 2.3.2	18 27	We recommend that security responsibilities be clearly defined and allocated in published guidelines and procedures.
4	1.3.3.1	19	We recommend that agencies ensure regular testing of security systems takes place and is properly logged.
5	1.3.3.2 2.3.3.3	19 28	We recommend evacuation procedures be clarified and tested for all sites regardless of staffing levels.
6	1.3.3.3 2.3.3.4	19 29	We recommend staff training needs be analysed to ensure staff exposed to significant risk are suitably trained to deal with situations that could arise.
7	1.4.1	20	We recommend consideration be given to minimising the risk presented to staff when working alone.
8	1.4.1	20	We recommend cash management procedures be incorporated into the risk assessment process and regularly reviewed.
9	1.5.1 2.5.1	21 31	We recommend all incidents be reported with details recorded in a register for review and risk assessment purposes and that explicit management action is taken.
10	1.5.2 2.5.2	22 33	We recommend security incidents be reviewed to identify systemic problems and develop strategies to treat risk.
11	2.3.1	26	We recommend a consistent and refined set of procedures and guidelines be developed that can be adapted and used at each school and library site.
12	2.3.3.1	28	We recommend priority be given to finding methods to implement sharing of security issues and solutions between responsible staff at sites operated by the department.

13	2.4.1	30	We recommend library staff have a secure work area at each library where possible.
14	2.4.2	31	We recommend the need for after-hours alarm systems be reviewed at library sites, where practical.
15	2.5.1	32	We recommend that the schools' security alarm monitoring database be improved to clearly distinguish false alarms and maintenance of alarm systems be improved to reduce the number of false alarms generated. The database should also include reporting of incidents that occur during school hours.
16	3.3.	37	We recommend more duress alarms be installed at the Department of Emergency Medicine (DEM) to ensure they are accessible to staff throughout the DEM.
17	3.3.	38	We recommend a monitor be placed in the waiting area at DEM so that the public are aware that they are under camera surveillance.
18	3.3.3.3	38	We recommend aggression management training for all nursing staff at DEM.

Management response

Department of Primary Industries and Water,
***Service* Tasmania**

I refer to your correspondence dated 7 September in relation to the above audit and thank you for the opportunity to comment on its recommendations as they relate to the *Service* Tasmania shop outlets.

I am aware that officers of my agency have already provided you with initial comments on an earlier draft Report, which we understand you have taken into consideration. As such I will limit my comments to the general thrust of the report.

Overall, I am of the view that the report and its recommendations are appropriate and reflect the current situation regarding security arrangements associated with the *Service* Tasmania shops.

The Department of Primary Industries and Water recognises the importance of ensuring an appropriate level of security for its shop premises and commissioned an independent consultant to review the current arrangements and practices relating to both Occupational Health and Safety and to shop security. It is interesting to note that the consultants report, in addition to the OH&S issues, made mention of the majority of matters raised in your report.

The department is currently assessing all the recommendations of both reports with a view to determining appropriate actions to implement their findings. Where this is not possible, we will take appropriate action to mitigate our exposure and that of our staff and the public. This review also will clearly define and allocate responsibilities for the actions identified.

I anticipate that the review process and the implementation of appropriate actions, including revised procedures, will be completed by the 30 June 2008 with a number being of an ongoing nature.

In conclusion I note that the overall findings of your review indicate that the general standard of security of *Service* Tasmania Shops is satisfactory. I concur with your general observation that with further refinement of our procedures we will be able to improve our overall security to preserve a safe environment for our staff and customers.

Department of Education, Schools and Libraries

The Department of Education welcomes the findings of the Report and the opportunity to comment on the key recommendations. The Report has successfully highlighted a range of issues that are of significance to this Department and has made a series of recommendations which are generally consistent with the Department's current plans for improvements in security.

The Department is planning to undertake a review of processes associated with facilities management and communication between sites and central office. Security risk analysis, policies, procedures and guidelines will form part of this process and the recommended principles of consistency and adaptability will be pursued. The review will be used as an opportunity to consider existing documented guidelines and procedures that are currently maintained on the Department's internal intranet site. Security responsibilities will also be considered as will the associated training needs.

The Report highlights the importance of effective communication on an issue such as security in a large decentralised organisation. The dispersed nature of the Department's schools and libraries and the differing scale of individual operations makes it difficult to achieve reliable communication networks and to fully standardise the management of security. However a range of strategies will be considered, including:

- the improvement of web-based resources;
- the incorporation of security issues on agendas at appropriate forums where staff with like responsibilities can share their experience and practices; and
- the identification of security responsibilities on statements of duties.

The Report's observations about evacuation practices and the importance of appropriate staff having the necessary skills in security practices and the operation of security equipment are noted. These will also inform the Department's review.

The Report's recommendation regarding the need for a secure work area in all library locations will be considered, although the practicality and the demonstrated need for such a strategy in the smallest of libraries may preclude full implementation of such a strategy.

Alarm systems will similarly be considered on a demonstrated needs basis. The current review of contracted security services is aimed at improving the quality of guard services and overall contract management arrangements which include improved reporting processes between guards, sites and central office; and the maintenance of alarm systems as this often varies from site to site. It is believed that better reporting arrangements with security contractors and the ongoing development of an electronic security monitoring and reporting system will assist the Department to develop a data store that can guide the development of relevant strategies to mitigate further security risks.

Department of Health and Human Services, Hospitals

The Department welcomes the findings of the audit in its recognition that the standard of security at the Department of Emergency Medicine was satisfactory and the recommendations for improvement are accepted. The recommendations will be reviewed with all Hospital CEOs through the formal audit improvement plans managed by the agency's Risk Management and Audit Committee.

The recommendations relating to duress alarms and use of monitors in DEM will be reviewed with hospital management to identify additional work that may be appropriately undertaken. Security is kept under active review in all high risk areas and improvements made progressively.

Since the audit occurred the new DEM has opened at the Royal Hobart Hospital and planning for the new $12 million DEM development at the Launceston General Hospital is underway. Security is an integral part of overall planning for these facilities.

In regard to aggression management training hospitals are continually developing training. The findings will be reviewed with hospital CEOs to assess the appropriate scope of coverage for training programs.

This page left blank intentionally

Introduction

Introduction

Background

In the compliance audit *Building Security* (Special Report No 60 of May 2006) we reviewed the effectiveness of security arrangements at selected government occupied office buildings that were not generally accessible to the public. The audit reported here, *Public building security*, focussed on physical security at buildings that have a high degree of public access.

Some of these facilities, such as hospitals, are physically difficult to secure against the risk of intruders, with large numbers of the general public having or requiring access for extended periods of time and at all hours. Other facilities, such as *Service* Tasmania sites or libraries, are only open during conventional or prescribed office hours perhaps making it easier for management to implement controls enhancing security.

Departmental Secretaries have an ethical and legal responsibility to adopt sound security management practices to protect their customers and staff, ensure privacy of information and safeguard assets. Effective security of public sector buildings is essential to ensure staff and property are protected from threats such as:

- unauthorised physical access
- theft of assets and personal property
- assaults on staff and visitors
- wilful damage including arson, graffiti, vandalism and damage from burglary
- misuse of assets, fraud and sabotage.

Security practices vary between departments according to the risk profile and nature of each site. Nonetheless, the following security management practices are widely applicable

- risk management
- establishing and maintaining the security environment
- recording and monitoring of security incidents.

Our findings on how departments have implemented these practices follow in the site-specific chapters of this Report.

Objective

The objective of the audit was to ascertain whether departments had adequate physical security procedures in place at the operational level to meet their obligations.

Scope

We reviewed physical security arrangements at the operational level at the following departments:

- Primary Industries and Water (DPIW) — *Service* Tasmania outlets
- Education (DoE) — schools and public libraries
- Health and Human Services (DHHS) — public hospitals.

The audit concentrated on physical security in selected buildings where public access is frequent.

Criteria

The criteria that we applied were:

- understanding the security threat using risk assessments to identify risks and vulnerability
- establishing and maintaining the security environment with:
    - policies and guidelines
    - allocation of security responsibilities
    - implementation of specific security measures
- keeping tabs on crime through:
    - adequate record keeping
    - regular review and monitoring.

Audit methodology

Our audit was conducted at the selected agencies by:

- using questionnaires to ascertain current status of the security profile
- conducting interviews with responsible staff
- conducting reviews of existing policy and procedures documentation
- conducting walkthroughs to test integrity of security arrangements

- comparing existing security arrangements with the risk management standard
- performing informal staff surveys.

Due to the complexities involved, we consulted the Department of Police and Emergency Management (DPEM) to assist with this audit.

Timing

Planning of the audit commenced in May 2006. The fieldwork was conducted from December 2006 through to April 2007 with this Report finalised in October 2007.

Resources

The total cost of the audit excluding report production costs was approximately $110 000.

1 *Service* Tasmania

1 *Service* Tasmania

1.1 Introduction

There are 26 *Service* Tasmania shops located in metropolitan and rural centres in the three regional areas around the state providing one-stop public access to government transactions, services and information. *Service* Tasmania commenced operating in 1997 and shop operations are administered by DPIW.

Aspects of *Service* Tasmania sites which influence physical building security management include the:

- shopfront style of operation
- receipting of money and the need for cash handling procedures
- need to facilitate discussion between staff and customers
- significant possibility or risk of angry customers.

Our findings were based on a judgement sample of six *Service* Tasmania locations, mixing rural and urban sites from around the state.

1.2 Security risk management

Security practices vary between S*ervice* Tasmania shops according to the security risk profile and nature of each site.

We used a questionnaire at each site to determine whether *Service* Tasmania undertook a security risk analysis to assess the current status of their security profile. We expected to find evidence of:

- identification and analysis of risk
- planned treatment of risk.

The S*ervice* Tasmania sites visited were subjected to an assessment by security consultants in 2003 and the majority of recommendations made at that time were implemented. That assessment was a valuable means of identifying and improving security arrangements. However, circumstances change and there has been no ongoing risk assessment since 2003.

In addition to the independent assessment in 2003, management at S*ervice* Tasmania assess workplace hazards by use of inspection checklists which include security, fire control and emergency procedures. However, the checklists provided had not been used since May 2005. In any event, the checklists are an aid to asset management and do not constitute a system of broader building security risk management as defined by the risk management standard. A current review by management of security checklists may improve risk analysis.

Recommendation 1

We recommend that a comprehensive security risk analysis that is regularly reviewed and updated be implemented at all public access sites.

1.3 Maintaining the security environment

Policies and guidelines provide the link between risk assessments and effective security measures. Responsibilities for security must be properly allocated to staff members. Procedures need to be fully implemented and appropriate to the security profile of the site at which they are applied.

1.3.1 Policies and guidelines

Security policies and procedures should be:

- based on risk assessment
- concise and unambiguous
- readily available and known by staff.

Service Tasmania does not have an overall security policy. However, security procedures and guidelines are available to staff on the departmental intranet covering areas such as:

- security awareness
- security equipment
- responses to crime
- testing of security equipment
- recording of incidents.

Interviews revealed a lack of staff awareness of these procedures. Staff knew the procedures were there, but admitted that they had not referred to them recently. To be considered effectively implemented, it is important that policies and procedures are known, comprehended and 'front of mind' by staff. A regular staff security information session could alleviate this problem.

We observed that some security procedures required updating. For example, procedures relating to the testing of closed circuit television equipment (CCTV) were specific to video tape recording equipment while all of the reviewed sites had computer hard drive recording systems installed. Also, the procedures must be specific as to when alarms should be tested to ensure that these tests take place and are logged.

Recommendation 2

We recommend details of security policies and guidelines be effectively communicated to staff and appropriate procedures be kept up-to-date and tested regularly.

1.3.2 Security responsibilities

Responsibilities should be suitably allocated to ensure that security measures once implemented are adequately maintained. We would expect to find such responsibilities detailed in procedures and examples include:

- general responsibilities with which all staff must comply
- specific duties assigned to staff categories (e.g. customer service officers, supervisors and managers).

We found that security responsibilities lacked definition, particularly at site level. This was indicated in the lack of implementation of testing procedures at some sites.

Recommendation 3

We recommend that security responsibilities be clearly defined and allocated in published guidelines and procedures.

1.3.3 Specific security measures

Specific security measures may vary from site to site, but we would expect to see that published procedures are properly implemented, including:

- testing of systems
- existence of comprehensive emergency procedures
- appropriate training for staff.

1.3.3.1 Testing of security systems

Service Tasmania procedures indicated that alarm system and duress alarm testing should be conducted 'regularly'. We found that only two of the six reviewed sites documented regular testing of the alarm system and of duress alarms while only one site documented CCTV system testing in their security logbooks.

Recommendation 4

We recommend that agencies ensure regular testing of security systems takes place and is properly logged.

1.3.3.2 Emergency procedures

We found that one third of the reviewed sites had no procedures for emergency evacuation and only half had ever held an evacuation drill. Because some rural sites may only have one staff member working for most of the opening hours, it is imperative that they know exactly what to do in the event of an emergency. Emergency procedures are currently under review by management.

Recommendation 5

We recommend evacuation procedures be clarified and tested for all sites regardless of staffing levels.

1.3.3.3 Staff training

Appropriate training for staff on security procedures must be provided on induction and refreshed regularly. However, we found that security training at *Service* Tasmania had been sporadic. 'Difficult Customers Made Easier' sessions were conducted in early 2006 and training regarding armed hold-up in 2003. Some staff members interviewed were satisfied with the training received during the induction process and with specific training on handling difficult customers. Others observed that the training was too generic and not specific to *Service* Tasmania situations. Some had not had any security training. Staff told us that security procedures were covered during induction but we could find no reference to security procedures in the induction manual.

Recommendation 6

We recommend staff training needs be analysed to ensure staff exposed to significant risk are suitably trained to deal with situations that could arise.

1.4 Controlling physical access

Control of physical access to buildings is essential to providing a safe and secure working environment for staff and the general public. Government buildings used by the public should:

- have clear delineation between areas the public use and secure work areas for staff only
- be protected after-hours
- have restricted access to confidential records.

1.4.1 Public and work areas

At *Service* Tasmania shops the level of access control was satisfactory. All sites visited had keypad or key card doors restricting access to non-public work areas. Registers in the security logbooks listed the holders of the door codes, swipe cards and keys. However, no procedure existed for changing the door codes on a regular basis.

The only other potential weaknesses noted were low counter heights, observed at two rural sites. Low counters did not provide sufficient separation between customers and staff and the vulnerability increases when staff are rostered to work alone.

The lack of an effective escape route posed a risk at two shops, since staff could potentially be trapped by aggressive customers. That situation was worsened by one of these sites not having a rear door from the work area. At the other site, the rear door opened to a corridor that was accessible from the front door of the office.

Recommendation 7

We recommend consideration be given to minimising the risk presented to staff when working alone.

Two of the larger *Service* Tasmania shops had floor plans that forced cash drops to be transported across the public area. We appreciate that this problem was caused by the design of the office layout, but recommend that a solution be investigated.

A recent reported security incident at another *Service* Tasmania shop involved a missing $3 000 cash drop. While cash management procedures generally were satisfactory, the abovementioned case highlights the need for ongoing review.

Recommendation 8

We recommend cash management procedures be incorporated into the risk assessment process and regularly reviewed.

1.4.2 After-hours alarms

Service Tasmania sites were satisfactorily protected after-hours by monitored alarm systems.

1.4.3 Access to confidential records

Controls to restrict access to confidential records were satisfactory at *Service* Tasmania sites.

1.5 Security incidents

Successful identification and treatment of risk depend on collection and review of security incidents as they occur. The security incident reporting system measures the effectiveness of changes to security procedures.

1.5.1 Record keeping

Maintaining and using information about security incidents is essential to sound security management. Data should be of a quality that ensures:

- effective response to systemic security issues
- monitoring of changes made to security procedures
- incidents (both after-hours and during work hours) are recorded.

The reported rate of security incidents for *Service* Tasmania shops was fourteen security-related incidents for the calendar year 2006 across 26 sites.

We were advised that staff members are encouraged to report all incidents, although some staff indicated that some incidents may be seen as an occupational hazard and not reported. For example, at a busy site abusive behaviour from customers occurring more frequently might be tolerated by staff and not reported.

We found no centralised register or database existed to facilitate review of security incidents over time.

Despite these findings, we noted that management dealt with reported incidents effectively and sensitively and staff felt supported by their Area Managers. However, one third of the staff members we interviewed stated that they did not feel safe at work.

Recommendation 9

We recommend all incidents be reported with details recorded in a register for review and risk assessment purposes and that explicit management action is taken.

1.5.2 Monitoring and reviewing

Monitoring and reviewing should:

- apply at both at the departmental and organisational unit level
- provide a systemic process for implementing changes
- ensure proactive changes to security policy and practice.

Of the fourteen security-related incidents mentioned in section 1.5.1, twelve involved difficult behaviour by customers, one theft by a customer and one cash management procedural matter.

Improvements were made to security practices and procedures as a result of the 2003 security report mentioned in section 1.2. In addition, an Occupational Health and Safety review by external management consultants is currently underway that may invoke some changes to security procedures.

Recommendation 10

We recommend security incidents be reviewed to identify systemic problems and develop strategies to treat risk.

1.6 Conclusion

While there are some areas of concern, the standard of security at *Service* Tasmania shops was generally satisfactory. However, a proactive approach is required to maintain or reduce the reported incidence rate. The department needs to ensure that site management applies consistent, effective procedures and solutions to security issues to preserve a safe environment for staff and the public.

2 Schools and libraries

2 Schools and libraries

2.1 Introduction

The Department of Education (DoE) manages the state's public schools and libraries. That task is a large one encompassing 215 government schools (that cater for 67 000 students) and 46 libraries, ranging from larger metropolitan sites to smaller branch and community sites.

Schools necessarily provide an open environment, readily accessible to the public. Difficulties regarding physical building security arise through out-of-hours vandalism, inappropriate access to buildings during the day and occasional difficult behaviour by parents or guardians of students.

Libraries must serve customers during opening hours and can face problems in dealing with difficult behaviour by customers.

Our findings are based on a review of a judgement sample of six schools including primary, secondary and colleges and six libraries, spanning rural and urban sites around the state.

2.2 Security risk management

We tested whether schools and libraries had undertaken a security risk analysis to identify risks and vulnerability. A questionnaire was used at each site to determine the current status of their security profile and we expected to find evidence of:

- identification and analysis of risk at a site level
- planned treatment of risk.

We found that the DOE has documented a commitment to risk management and has established the Risk Management Committee and the Risk Reference Group as part of its overall governance framework. Information presented on the department's intranet was reviewed and we concluded that the templates and direction given were thorough and compliant with the risk management standard but that security risk management has still to be explicitly addressed.

School and library management informed us that Risk Reference Group is overseeing a review aimed at developing a departmental risk management strategy referred to as the Roadmap Consultancy. Therefore we anticipate the adoption of risk management processes for security.

Specific findings were:

Schools

From interviews conducted on our visits to schools, it was apparent that no sites were as yet applying risk management to building security. No evidence was found that the materials and processes promoted on the department's intranet were being used.

Libraries

Similarly, none of the library sites tested had a risk management process for security. Security and risk assessors had performed a security review of heritage collections in 2006. We support the recommendation made in that review to develop an organisation-wide security management plan, using a risk management process.

As stated in Recommendation 1:

> We recommend that a comprehensive security risk analysis that is regularly reviewed and updated be implemented at all public access sites.

2.3 Maintaining the security environment

Policies and guidelines provide the link between risk assessments and effective security measures. Responsibilities for security should be properly allocated to staff members. Procedures need to be fully implemented and appropriate to the security profile of the site at which they are applied.

2.3.1 Policies and guidelines

Policies and guidelines provide the means by which risk assessments are linked to appropriate and cost effective security measures. We would expect to find that security policies and procedures are:

- based on risk assessment
- concise and unambiguous
- readily available and known by staff.

DoE staff can access the intranet for information regarding security and risk management. Policies, procedures and guidelines available from this information service cover topics such as:

- security guidelines
- emergency action guide
- difficult customers and critical incidents
- fire evacuation procedure template

- supply, installation and maintenance of security systems
- risk management guide and templates.

However, as noted previously, there is no specific policy or guide dealing with building security. Instead, the department has a policy of devolution regarding building security management and responsibility.

For policies and procedures to be effectively implemented it is important they are known, comprehended and 'front of mind' for staff. Interviews revealed a lack of staff awareness of these procedures; staff knew the procedures existed, but admitted they had not referred to them recently. The specific situation:

Schools

School principals are responsible for and develop security procedures at school sites. We concur that schools should have site-dependent security considerations, responsibilities and management arrangements in place, but found that the schools we visited had varied and sometimes limited written procedures for dealing with building security. Security incidents that arose and the solutions that were implemented were not documented nor led to policy development.

Libraries

Implementation of security policies and development of procedures in libraries were matters also entrusted to staff at libraries with similar results.

Recommendation 11

We recommend a consistent and refined set of procedures and guidelines be developed that can be adapted and used at each school and library site.

To improve staff awareness of security procedures, as stated in Recommendation 2:

> We recommend details of security policies and guidelines be effectively communicated to staff and appropriate procedures be kept up-to-date and tested regularly.

2.3.2 Security responsibilities

We tested whether security responsibilities were suitably allocated to relevant staff to ensure that security measures did not lapse and expected to find these responsibilities detailed in security policies. It was expected that responsibilities should include:

- general duties with which all staff must comply
- specific duties assigned to staff categories (e.g. principals, school executive officers (SEOs), teachers, school attendants and library staff).

We found that responsibilities were well defined in documented emergency and evacuation procedures at schools and larger libraries. However, due to other site-specific procedural documentation being deficient or non-existent, other building security responsibilities were not specifically defined at many of the school and library sites we visited.

As stated in Recommendation 3:

> We recommend that security responsibilities be clearly defined and allocated in published guidelines and procedures.

2.3.3 Specific security measures

Specific security measures may vary from site to site, but we would expect to see that published procedures are properly implemented. These include:

- sharing of effective solutions to security issues
- constructive use of outside security expertise
- comprehensive emergency procedures
- appropriate training for staff.

2.3.3.1 Sharing of security solutions

Principals, SEOs and library staff across the state have been faced with similar security challenges. We found examples of effective solutions that could be used in other locations including:

- One of the schools visited uses a security beam in the quadrangle to detect intruders after-hours.
- One metropolitan library uses a youth worker, funded through the local council community development office, during times when youth behaviour is a problem.

Staff could acquire knowledge from each other regarding solutions to security problems if they had more opportunities to share. A knowledge base, perhaps on an editable intranet site, and face-to-face forums could contribute to this communication.

Recommendation 12

We recommend priority be given to finding methods to implement sharing of security issues and solutions between responsible staff at sites operated by the department.

2.3.3.2 Use of outside expertise

We were impressed by the presence of the on-site police officer at a college we visited. It is understood that police officers are in use at other colleges and have a positive role in:

- education
- breaking down barriers and establishing rapport between the police and young people
- dealing with incidents on site
- driver training
- building pride in the school.

Police involvement at site level and local police knowledge of the site does assist in implementing security strategies and effectively responding to incidents when they occur. Advice, site assessment and other relevant information are available from the Police and can be of benefit in improving security.

2.3.3.3 Emergency procedures

DoE has embarked on a review of evacuation procedures in consultation with Tasmania Fire Service, and supported schools and libraries in updating their procedures and completing the initial evacuation practices during 2005 and 2006. The program which includes the initial supervised evacuation drill was partially complete at the time of the audit site inspections.

Schools

Evacuation procedures and drills were satisfactory at the schools visited.

Libraries

We noted that two of the library sites visited had no evacuation procedures and four had not held evacuation drills. While some of these sites have only one staff member working for most of the opening hours, it is imperative that everyone know exactly what to do in the event of an emergency.

As stated in Recommendation 5:

> We recommend evacuation procedures be clarified and tested for all sites regardless of staffing levels.

2.3.3.4 Staff training

Training regarding operation of security systems and dealing with difficult clients should be consistent, cyclic, pertinent and comprehensive. We expected to find that all staff exposed to significant risk were suitably trained to deal with situations that could arise.

Schools

At schools, personal development training sessions are available to staff sessions have been held on behavioural management and dealing with difficult parents of students. Teachers have behavioural management as a component of their teacher training. However, this training did not address the use of security equipment. Training in the operation and use of security equipment would contribute to reducing the large percentage of alarm call outs that are due to human error (88% state-wide).

Libraries

Library staff at only three of the six sites visited had received training in handling difficult customers and conflict resolution. The responsibility to initiate and request training rested on staff members.

As stated in Recommendation 6:

> We recommend staff training needs be analysed to ensure staff exposed to significant risk are suitably trained to deal with situations that could arise.

2.4 Controlling physical access

Control of physical access to buildings is essential to providing a safe and secure working environment for staff and customers. Government buildings used by the public should:

- have clear delineation between areas the general public use and secure work areas for staff only
- be protected after-hours
- have restricted access to confidential records.

2.4.1 Public access and staff work areas

Schools

We noted that public access control for schools is complicated by the fact that the grounds are open areas the public can enter or traverse during and after school hours. Involvement with the local community through activities on school sites promotes greater public awareness of school security. We were informed that the continuing problems for schools involve undesirable activities resulting in mess, damage or theft.

Libraries

Branch libraries had staff work areas that could be accessed by the public. That exposure was compounded by the fact that staff at branch libraries mostly work alone. Phones are programmed to speed dial the local police station in an emergency but response times, especially in non-metropolitan areas, may not be immediate. Cordless phones are provided so that calls can be made away from the desk if necessary.

Library counters at the sites visited were well placed to provide best possible sight lines for staff and the space behind the counter was clearly delineated. Staff working alone are required to spend most of their time in public areas to effectively provide security for the collections and provide service to customers.

There is a specific public access difficulty at a major regional library. The central stairs of the building must remain unlocked, as they constitute a fire escape but in doing so allow public access to the work area in the basement where staff members are not always present. The server and computer equipment located there are exposed to malicious damage and items held in the workspace are susceptible to theft.

Recommendation 13

We recommend library staff have a secure work area at each library where possible.

2.4.2 After-hours alarms

Schools

School buildings are protected by monitored electronic alarms. The contracted security firm actions each alarm trigger and provides information about each incident into the departmental database. Schools are responsible for provision and maintenance of their alarm systems.

Libraries

The four branch libraries that we visited did not have after-hours alarm systems. Although only small amounts of cash are kept on site, the risk of break-in and vandalism of library property could have serious consequences.

Recommendation 14

We recommend the need for after-hours alarm systems be reviewed at library sites, where practical.

2.4.3 Access to confidential records

Controls to restrict access to confidential records were found to be satisfactory at schools and libraries.

2.5 Security incidents

Successful identification and treatment of risk are enhanced by collection and review of security incidents as they occur. Security incident reporting systems measure the effectiveness of changes to security procedures.

2.5.1 Record keeping

Maintaining and using information about security incidents is essential to sound security management. The data collected needs to be of a quality that ensures:

- breaches of security, both after-hours and incidents that occur during working hours are documented
- effective response to systemic security issues
- monitoring of changes made to security systems.

Schools

The monitoring contractor records triggers of after-hours security alarms at schools directly into the departmental database. We noted that the total number of security alarm triggers has doubled from 200 to 400 per month over the last three years. However, two problems were evident.

First, there is a high level of false alarms (88% — see section 2.3.3.4) largely due to human error (e.g. staff not setting alarms at the end of the day or accidentally triggering alarms at opening). Secondly, when security patrols check the premises they often fail to indicate the outcome. The result is that the value of the data provided is compromised.

Analysis of data from categories more likely to yield genuine alarms, namely: break-glass alarm, premises insecure, external vandalism, break-and-enter, intruder alert and duress or hold-up, revealed an increase from 20 to 40 incidents per month over the same period.

During school hours, security-related incidents are only reported when damage or injury occurs. It would be more useful if all security incidents were appropriately and consistently reported for analysis purposes.

At the schools we visited, principals and SEOs were committed to, and effective in, dealing with incidents brought to their attention. It was found that responses to incidents were not documented other than by the resulting funds expended or works instigated. No centralised register of actions and responses relating to security existed.

Recommendation 15

We recommend that the schools' security alarm monitoring database be improved to clearly distinguish false alarms and maintenance of alarm systems be improved to reduce the number of false alarms generated. The database should also include reporting of incidents that occur during school hours.

Libraries

Library security incidents during operating hours are reported and stored on paper-based incident forms. It was apparent that the number of incidents reported was not high. Prior to commencing this audit, one library was described as the security 'hot spot'. When we visited we were advised of on-going problems with difficult behaviour and occasionally customers were using the library toilets to inject drugs. Despite this, only eight incident reports were noted for the period supplied and none were for the purported drug-related problems.

Security incident reporting requires consistent standards. For example, an incident that involves an abusive client may be seen as an occupational hazard by some staff members and not reported.

Reported incidents appeared to be dealt with effectively and sensitively by management. Library staff felt supported by their managers. One third of the staff members we interviewed at libraries, however, indicated that they did not feel safe at work.

As stated in Recommendation 9:

> We recommend all incidents be reported with details recorded in a register for review and risk assessment purposes and that explicit management action is taken.

2.5.2 Monitoring and reviewing

Monitoring and reviewing should:

- be practised at both at the departmental and organisational unit level
- be a systemic process for implementing changes
- ensure that changes made to security policy and practice are pro-active.

Schools

We were concerned by our finding that security incidents at schools during work hours were not being effectively reviewed. Schools often dealt with incidents individually without necessarily reporting them. The development of an online incident reporting system would enable recording of all incidents for monitoring and reviewing.

Libraries

Security incidents that occur during work hours at libraries are reported using a paper form. These are filed at State Library head office after required action is taken. No review of incidents is performed.

As stated in Recommendation 10:

> We recommend security incidents be reviewed to identify systemic problems and develop strategies to treat risk.

2.6 Conclusion

While there were a number of areas of concern, the standard of security at schools and libraries was generally satisfactory. The incident rates reported were low, but tending to increase and a proactive approach is required. The department needs to ensure that site management applies consistent procedures and solutions to building security risks. This will provide for a safer environment for staff and for the public.

This page left blank intentionally

3 Hospitals

3 Hospitals

3.1 Introduction

Public hospitals are administered by DHHS and are covered by its security policy. Within this policy, each hospital site manages and maintains its security systems and personnel.

Hospitals have many requirements regarding building security and public access. Our findings are based on a review of a Department of Emergency Medicine (the DEM) at a major general hospital. DEMs have unique security challenges including:

- providing a secure area for treatment
- 24-hour a day, 7 days a week access
- difficult behaviour by some patients and visitors
- protection of the privacy and dignity of patients under care.

3.2 Security risk management

Documenting a commitment to risk management, the department's Security Policy preamble states that, 'Security risks will be assessed and treated in accordance with Australian Standard — Risk Management (AS 4360:1999)'. Although a security risk assessment was completed in the DEM about four years ago, there was no evidence of ongoing risk treatment and mitigation. Risk management as defined by the risk management standard is a continual process.

As stated in Recommendation 1:

> We recommend that a comprehensive security risk analysis that is regularly reviewed and updated be implemented at all public access sites.

3.3 Maintaining the security environment

Policies and guidelines provide the link between risk assessments and effective security measures. Responsibilities for security must be properly allocated to staff members. Procedures need to be fully implemented and appropriate to the security profile of the site at which they are applied.

3.3.1 Policies and guidelines

We concluded that the DHHS security policy, an overarching document that can be applied throughout sites controlled by it, is satisfactory. The Emergency Management Protocols, as they relate to building security and personal safety, are also in our view satisfactory.

In addition, security policy, procedures and staff awareness of them at the DEM proved satisfactory.

3.3.2 Security responsibilities

We tested whether security responsibilities were suitably allocated.

Results showed that security responsibilities were satisfactorily delegated at the DEM. Security policy documents contained specific responsibilities and duties for:

- general requirements with which all staff must comply
- specific duties assigned to staff categories (e.g. nursing staff, orderlies and attendants, supervisors, medical staff and managers).

3.3.3 Specific security measures

Specific security measures put in place may vary from hospital to hospital, but we expected:

- appropriate security hardware to be in place
- comprehensive critical incident procedures
- appropriate training for staff.

3.3.3.1 Appropriate security hardware

Considering the high incidence of aggressive behaviour and the size of the DEM, staff need to be able to reach a duress alarm easily at all times. We found that at the DEM, two duress alarms were provided at the front counter and one at the nurses' station.

Portable units had been used, but proved problematic when staff had not registered that they were using one. Future security arrangements, we were informed, will negate the need for portable alarms.

There were three cameras in the DEM precinct including one in the waiting area with signage indicating that the area was under video surveillance. Despite this, a number of incidents had occurred in the waiting area which may indicate a need for a more obvious signal that the area is under surveillance.

Recommendation 16

We recommend more duress alarms be installed at the DEM to ensure they are accessible to staff throughout the DEM.

Recommendation 17

We recommend a monitor be placed in the waiting area at DEM so that the public are aware that they are under camera surveillance.

3.3.3.2 Emergency procedures

Emergency procedures for fire, bomb threat, personal threat, evacuation, and internal emergency were fully documented and regularly drilled.

3.3.3.3 Staff training

It is commendable that an aggression management program has been implemented at the DEM. This training is compulsory for security staff and medical orderlies and is performed annually. The Australian Nursing Federation has urged that all DEM nursing staff should receive the training as a compulsory and integrated component of a unit's formal accreditation framework. We support this recommendation.

Recommendation 18

We recommend aggression management training for all nursing staff at DEM.

3.4 Controlling physical access

Control of physical access to buildings is essential to providing a safe and secure working environment for staff and the general public. We expected to find that the DEM areas used by the public would:

- have clear delineation between areas the public use and secure work areas for staff only
- be protected after-hours
- have restricted access to confidential records.

3.4.1 Public and work areas

Measures in place to control the physical access to the DEM were satisfactory. Swipe card access was required to the treatment area.

3.4.2 After-hours alarms

After hours, the control room manages access to the waiting area by remotely unlocking the front doors.

3.4.3 Access to confidential records

Controls to restrict access to confidential records were satisfactory at the DEM.

3.5 Security incidents

Maintaining and using information about security incidents is essential to sound security management. The data collected needs to be of a quality that enables effective response to systemic security issues and to enable on going monitoring of changes made to security practices.

We expected to find a security incident reporting system that covered all the security related risks to which the DEM is exposed.

3.5.1 Record keeping

Breaches of security, both after-hours and incidents that occur during working hours should be documented to enable meaningful analysis and to facilitate effective review of measures put in place to improve security. The data collected needs to be of a quality that ensures:

- effective response to systemic security issues
- monitoring of changes made to security systems
- breaches of security, both after-hours and incidents that occur during working hours are documented.

Security incident reporting requires consistency in reporting standards.

We found that the requirements for incident reporting were satisfactory; being covered by the hospital security policy and the departmental publication 'Simple Guide to Incident Reporting'.

Management deals with reported incidents effectively and sensitively and staff at the DEM stated that they felt supported by management.

3.5.2 Monitoring and reviewing

We were looking for:

- a system of reviewing and monitoring security
- the existence of a systemic process for implementing changes
- evidence that changes made to security policy and practice were pro-active.

We found that security incidents were analysed effectively and comparisons were made to other hospital sites over the same time periods. Security incidents were effectively categorised for analysis purposes.

3.6 Conclusion

While there are some areas of concern the standard of security at the DEM was satisfactory.

4 Recent reports

Recent reports

Year	Special Report No.	Title
2002	40	Environmental management and pollution control
2002	41	Keeping schools safe
2002	42	Follow up of performance audits
2002	43	Oral health service: Something to smile about?
2002	44	Managing community service orders
2003	45	Business names and incorporated associations: What's in a name?
2003	46	Leave in government departments
2003	47	Public sector web sites
2003	48	Grants to the community sector
2003	49	Staff selection in government agencies
2003	50	Police response times
2004	-	Ex-gratia payment to the former Governor Mr R W Butler AC
2004	51	Special purpose and trust funds: Department of Health and Human Services
2004	52	Internal audit in the public sector
2005	53	Follow-up audits
2005	54	Compliance audits
2005	55	Gun control in Tasmania
2005	56	TT-Line: Governance review
2005	57	Public housing: Meeting the need?
2005	58	FBT, Payment of Accounts and Bridges
2006	59	Delegations in government agencies, Local government delegations and Overseas Travel
2006	60	Building Security and Contracts appointing Global Value Management
2006	61	Elective surgery in public hospitals
2006	62	Training and development
2006	63	Environmental management and pollution control act by local government
2006	64	Implementation of aspects of the *Building Act 2000*
2007	65	Management of an award breach and Selected allowances and nurses' overtime
2007	66	Follow-up audits June 2007
2007	67	Corporate credit cards
2007	68	Risdon Prison: business case

5 Future projects

Future projects

Performance and compliance audits that the Auditor-General is currently conducting:

Court waiting times The objective of this audit is to examine the efficiency and effectiveness of the management of court waiting times within the judicial process in Tasmania.

Endangered species/biodiversity Examines measures in place to protect native species and biodiversity in Tasmania.

Property in police possession Reviews management of confiscated and forfeited property by Tasmania Police.

Portable and attractive items Examines asset control activities at government departments with respect to items that are portable and attractive.

Creditor processing As a follow on from Special Report no. 58, which in part examined payment of accounts in agencies, this audit seeks to establish that the accounts payable processes within agencies are in accordance with Treasurer's Instructions.

Procurement This audit examines whether procurement by government departments is in accordance with applicable Treasurer's Instructions. This audit follows on from Special Report No. 34.

Key performance indicators To assess whether current key performance indicators are relevant and appropriate measures of effectiveness and efficiency of government performance as reflected in agencies' annual reports.