



# Audit Report in Vulnerability and Penetrating Testing

**INFORMATION DATA SECURITY SYSTEM**

**EyeD infocomm & Security Solutions**

---

Toa Payoh  
Singapore

[www.eyed.com.sg](http://www.eyed.com.sg)  
[enquiries@eyed.com.sg](mailto:enquiries@eyed.com.sg)

---

### Contents

Audit Scope and Methodology	1
Analysis of results	3
Control Category	4
Access Control Findings	6
Security Management Findings	8
What we do?	10
Recommendation of the Legislature	12

*Public entities rely heavily on information technology (IT) to achieve their missions and business objectives. As such, IT controls are an integral part of entity internal control systems. The Auditor General evaluates the effectiveness of entity controls over IT as a part of financial and operational audits.*

## Audit Scope and Methodology

---

### Executive Summary

We conducted a performance audit to assess information security in best practices to determine compliance with certain aspects of the security policy can be affected by vulnerabilities or possible loop holes to affect the data and server gain access.

### Financial Highlights

The Auditor General, in keeping with of the Financial Administration and Audit Act commissioned an audit of client to determine whether adequate systems, policies and procedures were in place in relation to client core activities, i.e. the provision of information and communication technology services and support to the beneficiary.

### Audit Focusing

Our audit focused on assessing the efficiency and effectiveness of client's general computer controls to ensure that systems, policies and procedures are in place to preserve the integrity and confidentiality of data as well as the continuity of various client's computer systems. This involved the review and testing of controls in the following areas:

- Physical and Environmental Security
- Access Controls and System/Network Security
- Business Continuity and Disaster recovery
- Change Management and Control
- Management of Human Resources and Corporate Governance

## What we done

The security gap analysis was conducted across 8 clients as part of our annual general computer controls audits. We assessed information security across all security categories defined within the international standard. There are essentially 12 areas the standards focus on with each area containing various categories.

The areas are:

- Physical and Environmental Security
- Security Policy
- Access Control
- Human Resources Security
- Organizing Information Security
- Communications and Operations Management
- IS Acquisition, Development and Maintenance
- Compliance
- Asset Management
- Information Security Risk Management
- Information Security Incident Management
- Business Continuity Management

Area	1	2	3	4	5	6	7	8
Physical and Environmental Security	Green	Green	Green	Green	Green	Green	Yellow	Green
Security Policy	Green	Green	Green	Green	Green	Green	Red	Green
Access Control	Yellow	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow
Human Resources Security	Green	Yellow	Green	Yellow	Green	Red	Yellow	Red
Organising Information Security	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow
Communications and Operations Management	Green	Green	Green	Green	Red	Yellow	Yellow	Yellow
IS Acquisition, Development and Maintenance	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Yellow
Compliance	Green	Green	Green	Yellow	Red	Yellow	Yellow	Red
Asset Management	Red	Green	Yellow	Green	Red	Red	Yellow	Yellow
Information Security Risk Management	Red	Red	Red	Green	Green	Green	Red	Red
Information Security Incident Management	Red	Red	Yellow	Red	Red	Green	Red	Red
Business Continuity Management	Yellow	Yellow	Red	Red	Green	Red	Red	Red

Each area was assessed in terms of its effectiveness in meeting the standards and scored. We rated scores above 85 per cent to be effective, scores between 60 to 85 per cent as partially effective and below 60 per cent as ineffective. Those areas in the standard that were obviously not applicable to the clients we audited were not considered.

## Analysis of results

---

The standards provide guidance on how an organization should approach information security. The starting point is establishing what the security requirements are and assessing risk. Security requirements can be derived from three main sources which include

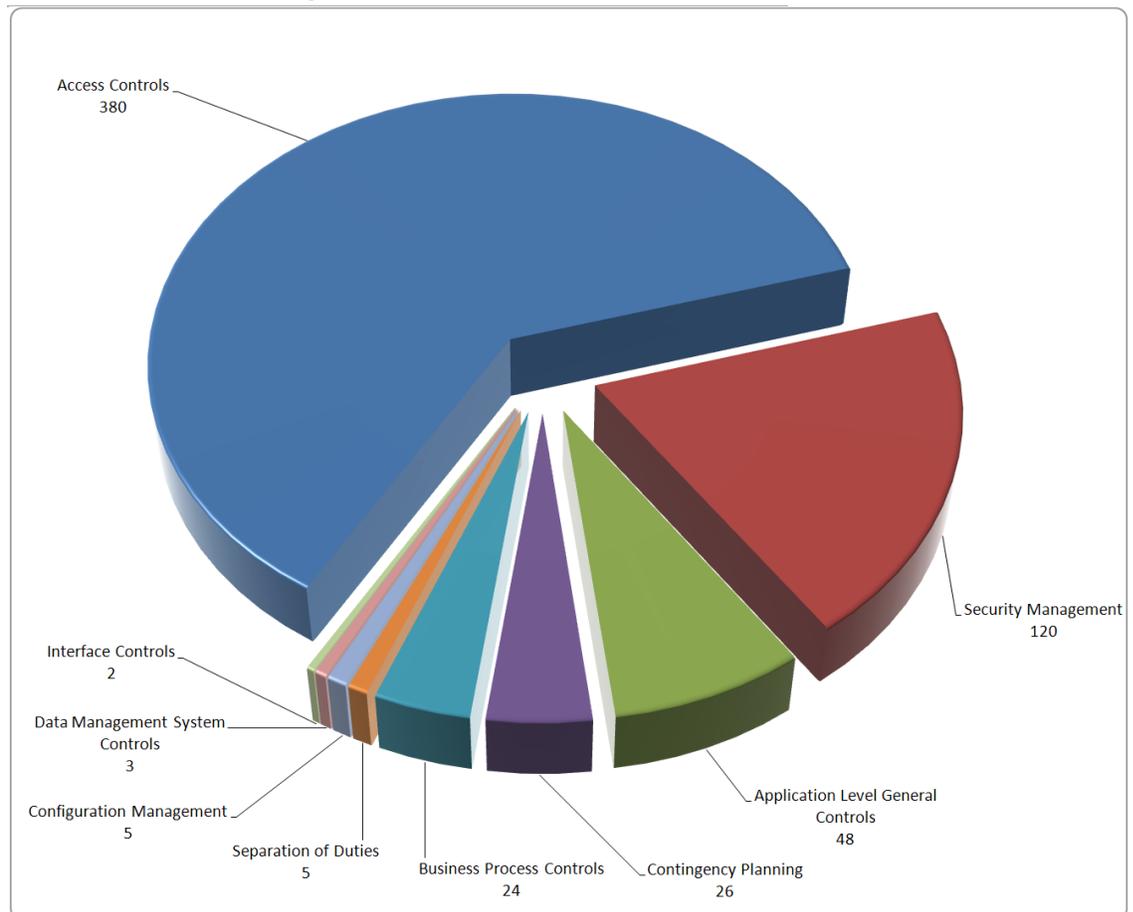
- (1) Assessing risks taking into account the overall business strategy and objectives.
- (2) The legal, statutory and regulatory requirements including contractors, service providers and partners.
- (3) The principles, objectives and business requirements for information processing to support operations.

Our analysis indicated that many of the clients are not taking these first steps by adopting a strategic approach to identifying and assessing risks. This can be seen in above table which shows that only half of the clients rated well in the Information Security Risk Management category. This is an important area of initial focus to identify, assess and treat risks and allows clients to take a strategic approach to managing information security. This can lead to clients wasting resources on areas of minimal risk while leaving critical areas exposed.

Clients should use their risk assessment to inform the development of business continuity and specific incident management plans. A sound information security policy is important for security governance and should also be informed by the initial risk assessment. Above table illustrates that clients that met the standards in these areas generally did better across all other areas. However a common failing was lack of business continuity management for information security. These plans help to ensure clients can recover or continue to function should a serious incident occur.

## Control Category

Control Category	Number of Findings
Access Controls	380
Security Management	120
Application Level General Controls	48
Contingency Planning	26
Business Process Controls	24
Separation of Duties	5
Configuration Management	5
Data Management System Controls	3
Interface Controls	2
<b>Total Number of Findings</b>	<b>613</b>



## General Controls

- **Security Management:** Controls providing assurance that security management is effective. Examples include a security management program, periodic risk assessments and validation, and security control policies and procedures.
- **Access Controls:** Controls providing assurance that access to data, software, equipment, and facilities is reasonable and restricted to authorized individuals.
- **Configuration Management:** Controls providing assurance that changes to IT system resources are authorized and systems are configured and operated securely and as intended.
- **Separation of Duties:** Controls providing assurance that incompatible duties are effectively separated.
- **Contingency Planning:** Controls protecting information resources, minimizing the risk of unplanned interruptions, and providing for the recovery of critical operations should interruptions occur.

## Business Process Application Controls

- **Application Level General Controls:** General controls, including the five types of controls listed above, operating at the business process application level.
- **Business Process Controls:** Automated and manual controls applied to business process flows, including controls over transaction data input, processing, and output and controls over master data.
- **Interface Controls:** Controls over the timely, accurate, and complete processing of information between applications and other feeder and receiving systems and the complete and accurate migration of clean data during conversion.
- **Data Management System Controls:** Controls used in data management systems, such as database management systems, middleware, data warehouse software, and data extraction and reporting software.

## Access Control Findings

Access controls limit or detect inappropriate access to IT resources, thereby protecting the IT resources from unauthorized disclosure, modification, and loss. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, modify, delete, or exfiltrate (remove) data or execute changes that are outside their span of authority.

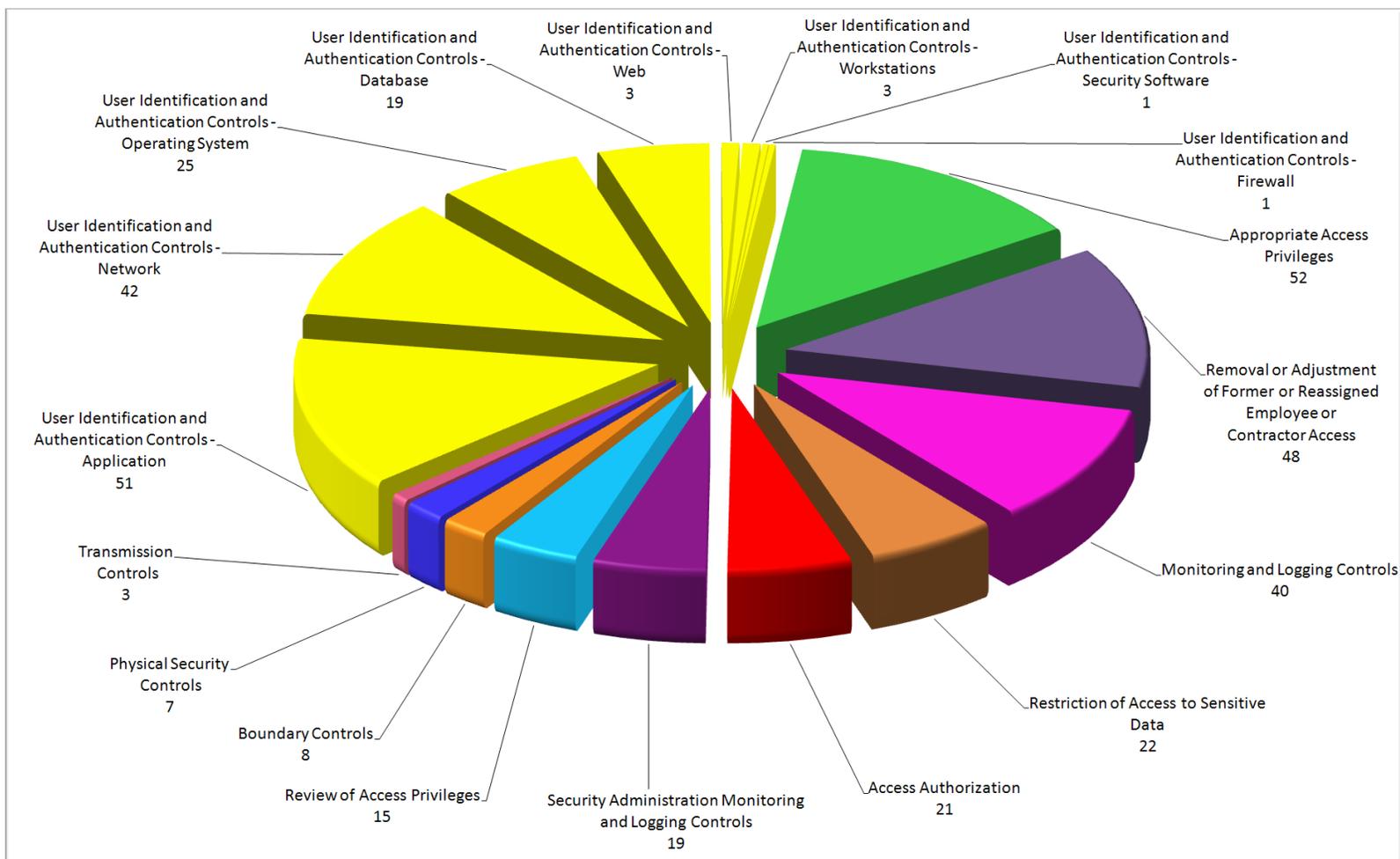
The following table and chart provide a breakdown of access control findings by the specific control technique needing improvement.

Access Controls – Control Techniques	Number of Findings	Number of Entities
<b>Appropriate Access Privileges</b>	52	45
<b>User Identification and Authentication Controls – Application</b>	51	44
<b>Removal or Adjustment of Former or Reassigned Employee or Contractor Access</b>	48	41
<b>User Identification and Authentication Controls – Network</b>	42	41
<b>Monitoring and Logging Controls</b>	40	28
<b>User Identification and Authentication Controls - Operating System</b>	25	25
<b>Restriction of Access to Sensitive Data</b>	22	20
<b>Access Authorization</b>	21	17
<b>User Identification and Authentication Controls – Database</b>	19	16
<b>Security Administration Monitoring and Logging Controls</b>	19	18
<b>Review of Access Privileges</b>	15	13
<b>Boundary Controls</b>	8	8
<b>Physical Security Controls</b>	7	6
<b>Transmission Controls</b>	3	3
<b>User Identification and Authentication Controls - Web</b>	3	3
<b>User Identification and Authentication Controls - Workstations</b>	3	3
<b>User Identification and Authentication Controls - Security Software</b>	1	1
<b>User Identification and Authentication Controls - Firewall</b>	1	1

Total Number of Findings	380	333
--------------------------	-----	-----

Access Controls

Number of Findings by Control Technique



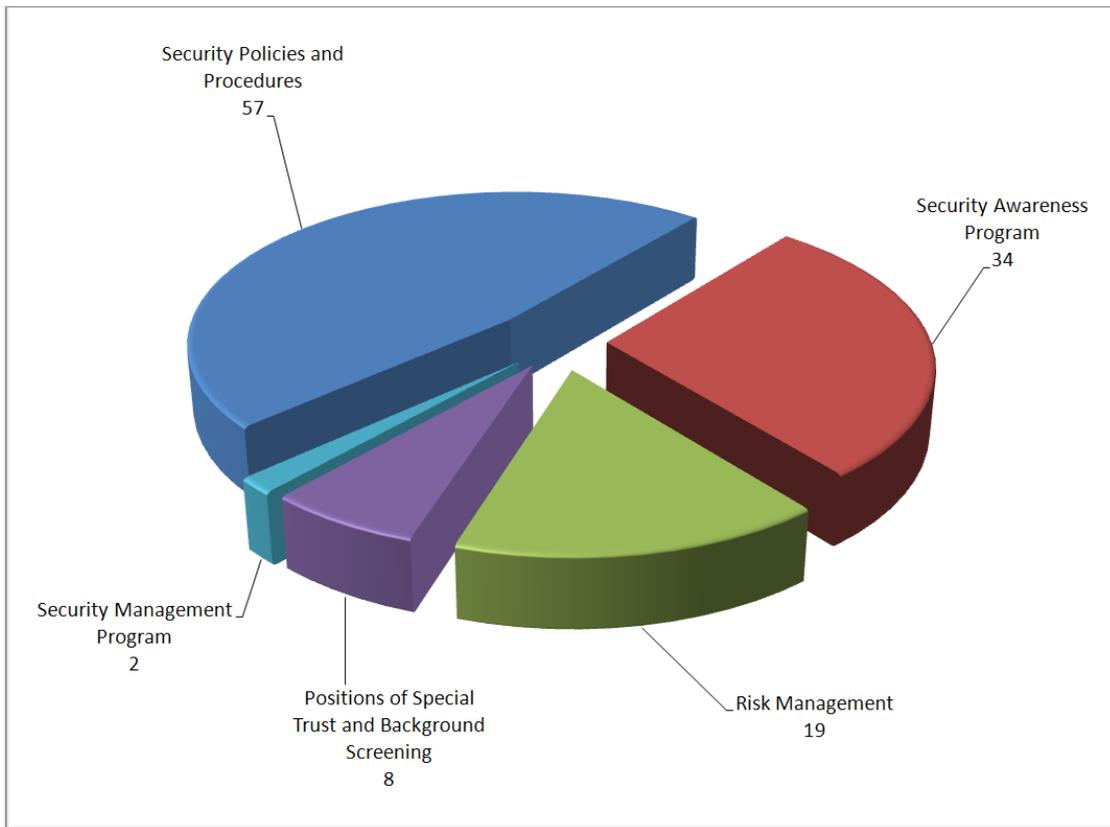
**Security Management Findings**

The effectiveness of an entity’s access controls and other aspects of IT security are dependent in part on the effectiveness of its overall security management. An entity wide security management program is the foundation of a security control structure and a reflection of senior management’s commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures. Improvements in the overall IT security management of public entities would enhance their ability to identify, assess, and remedy deficiencies in IT security controls in a cost-effective manner. The following table and chart provide a breakdown of security management findings by the specific control technique needing improvement.

<b>Security Management – Control Techniques</b>	<b>Number of Findings</b>	<b>Number of Entities</b>
<b>Security Policies and Procedures</b>	57	48
<b>Security Awareness Program</b>	34	33
<b>Risk Management</b>	19	17
<b>Positions of Special Trust and Background Screening</b>	8	8
<b>Security Management Program</b>	2	1
<b>Total Number of Findings</b>	120	107

**Security Management**

**Number of Findings by Control Technique**



## What we do?

---

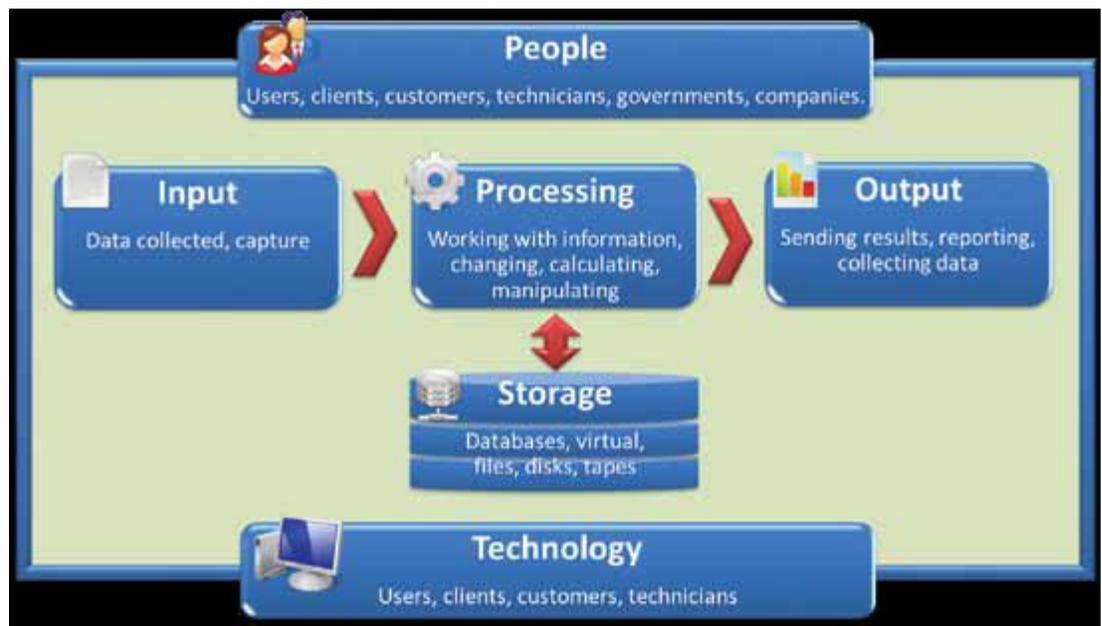
We reviewed five key business applications at four clients. Each application was selected on the basis of the significant impact on the client or the public if the application was not managed appropriately.

Our application reviews involve an in-depth focus on the step by step processing and handling of data. Our main purpose for reviewing computer applications is to gain assurance that:

- **Policies and Procedures** – appropriate policies and procedures are in place to support reliable processing of information
- **Data Preparation** – controls over the preparation, collection and processing of source documents are accurate, complete and timely before the data reaches the application
  - **Data Input** – data entered into the application is accurate, complete and authorized.
  - **Data Processing** – is processed as intended in an acceptable time period
  - **Data Output** – output including online or hardcopy reports, are accurate and complete
- **Interface Controls** – controls are suitable to enforce completeness, accuracy, validity and timeliness of data transferred
- **Master File Maintenance** – controls over master file integrity are effective which ensure changes are approved, accurate and complete
- **Audit Trail** – controls over transaction logs are in place which ensure transaction history is accurate and complete

- **Segregations of Duties** – no staff performed incompatible duties
- **Backup and Recovery** – the system/application can be recovered in the event of a disaster.

Figure represents the main elements: people, process, technology and data that are the focus of our application reviews. In consideration of these elements, we follow the data from input, processing, storage to outputs.



### Recommendation of the Legislature

---

Maintaining effective internal controls, including IT controls, is an important management responsibility. As shown in the summarizations of IT control issues provided above, the nature and extent of IT audit findings noted in our audit reports issued previously and the percentage of repeated findings indicate that information security programs have not yet been fully or effectively implemented for numerous entities and that entity management, those charged with governance, and other stakeholders should place an increased emphasis on improving the security and control of public data and IT resources. Without effective IT security and control practices, controls may continue to be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied.

We recommend that the Legislature consider establishing a workgroup composed of applicable stakeholders to study and make recommendations for strategies to promote an appropriate level of security of data and IT resources for entire clients. The workgroup should include representatives from the department of security auditing, the penetrating testers, white hat, and grey hat attackers. Matters to be addressed by the workgroup could include strategies in the following areas: promoting information security awareness, standards, and guidelines; conducting security planning and risk analyses; establishing cost-effective IT security and control practices to reduce identified security risks; and ensuring the conduct of periodic internal audits and evaluations of information security programs.

### Conclusion

This report has outlined how we went about conducting the audit of information systems, reported the outcome of our audit and described what we will do as a result of the audit (our priorities). Ninety per cent of the clients we reviewed had serious gaps in their management of information security when assessed against better practice international standards. Many of the clients sampled are not adopting a strategic approach to identifying and assessing risks. In the absence of a strategic approach client may be wasting resources on areas of minimal risk while leaving critical areas exposed. This result suggests a lack of understanding and implementation of good information security practices across the Public Sector and of systems being put at unnecessary risk.