Audit Report in Vulnerability and Penetrating Testing

INFORMATION DATA SECURITY SYSTEM

EyeD infocomm & Security Solutions

Toa Payoh
Singapore

www.eyed.com.sg
enquiries@eyed.com.sg

Contents

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 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

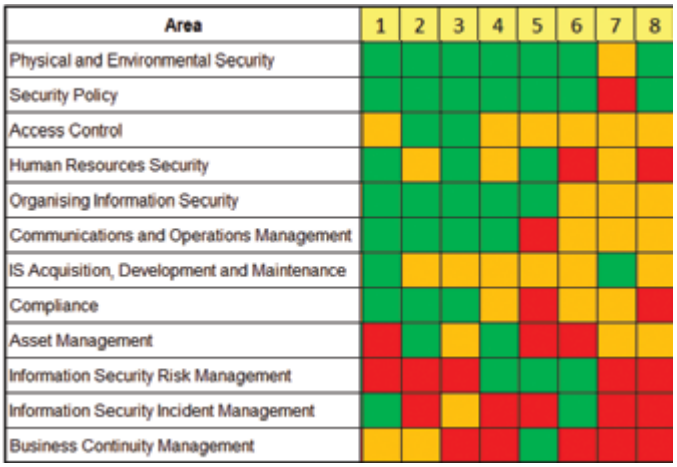
Audit Scope and Methodology

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



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.

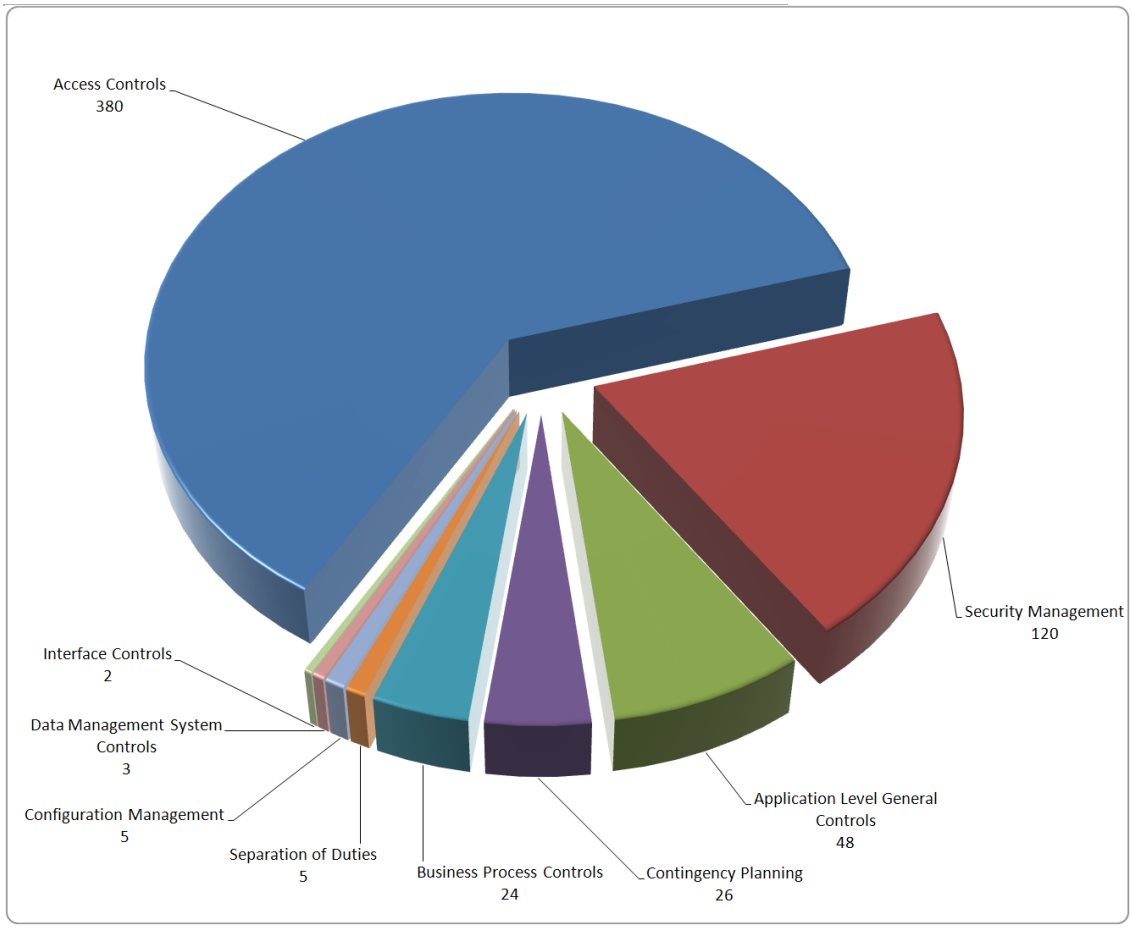
(3) The principles, objectives and business requirements for information processing to support operations.

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
Total Number of Findings	613



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

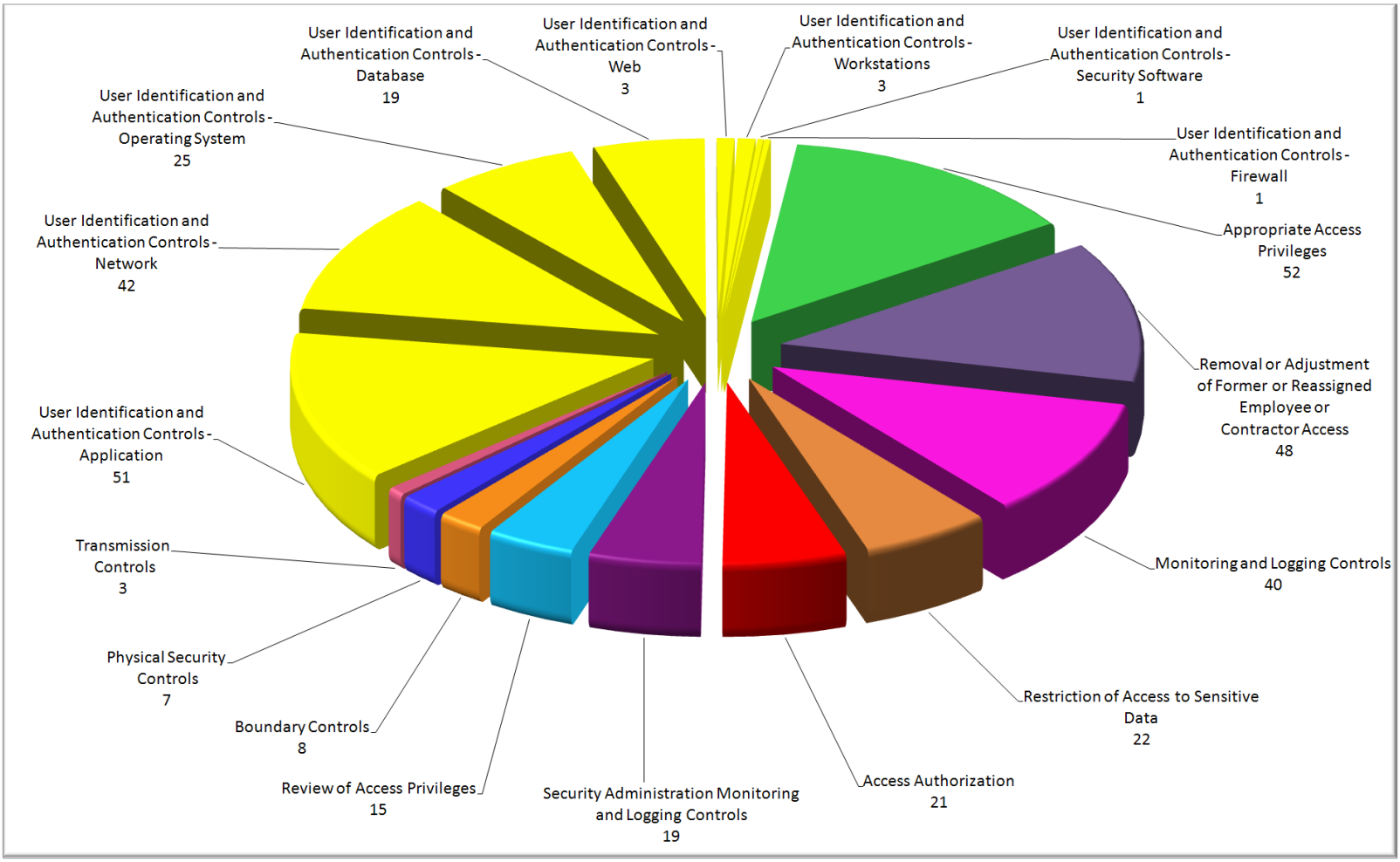
Access controls limit or detect inappropriate access to IT resources, thereby protecting the IT resources from unauthorized disclosure, modification, and loss. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy 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
Appropriate Access Privileges	52	45
User Identification and Authentication Controls – Application	51	44
Removal or Adjustment of Former or Reassigned Employee or Contractor Access	48	41
User Identification and Authentication Controls – Network	42	41
Monitoring and Logging Controls	40	28
User Identification and Authentication Controls - Operating System	25	25
Restriction of Access to Sensitive Data	22	20
Access Authorization	21	17
User Identification and Authentication Controls – Database	19	16
Security Administration Monitoring and Logging Controls	19	18
Review of Access Privileges	15	13
Boundary Controls	8	8
Physical Security Controls	7	6
Transmission Controls	3	3
User Identification and Authentication Controls - Web	3	3
User Identification and Authentication Controls - Workstations	3	3
User Identification and Authentication Controls - Security Software	1	1
User Identification and Authentication Controls - Firewall	1	1
Total Number of Findings	380	333

Access Controls

Number of Findings by Control Technique



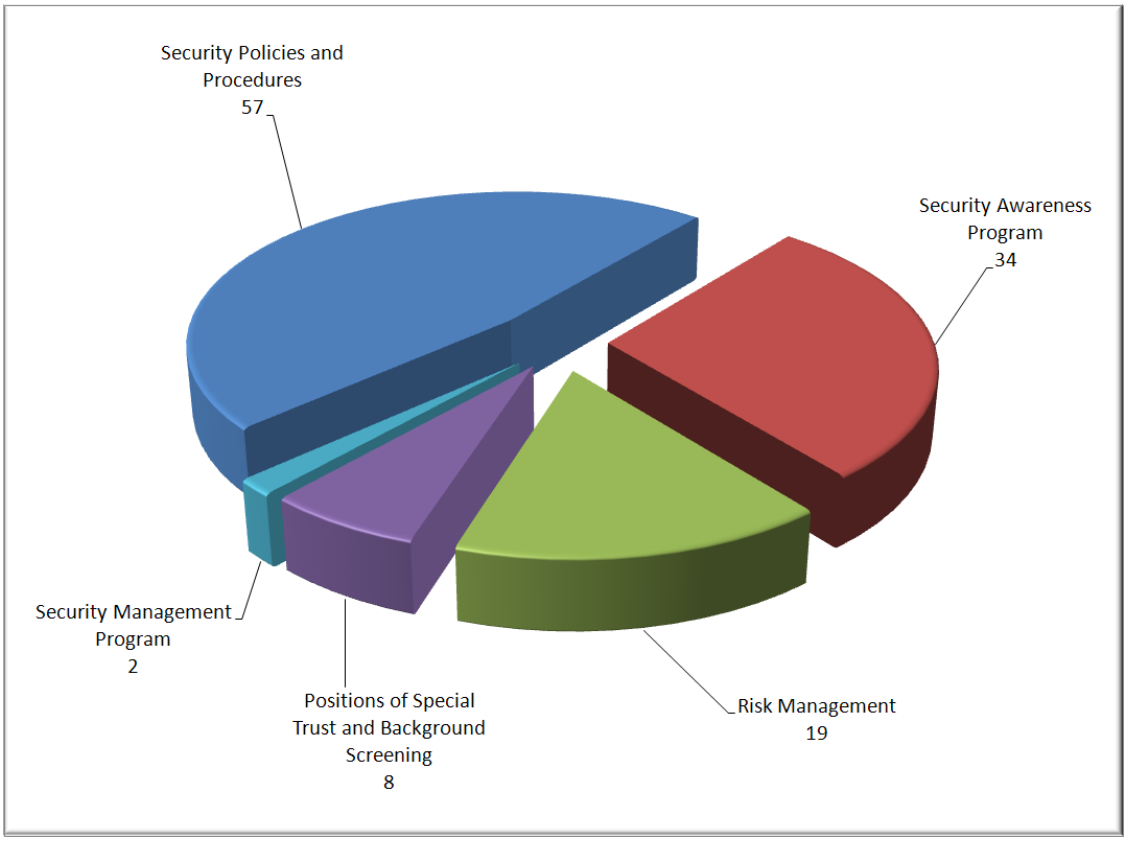
Security Management Findings

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.

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

Security Management

Number of Findings by Control Technique



JD Edwards monitoring methods

A number of third party OS400/I5OS tools for database audit exist and the OS itself has its own database change recording mechanism though Journaling. However neither of these are designed to work seamlessly with JD Edwards. This can make setup more complicated (file/environment identification etc.) and create additional integration work for JDE customers. Third party tools will obviously generate additional costs both in terms of acquisition and implementation.

Journaling itself has a very wide scope and does not exist to simply record database updates. It has been designed to cover amongst other things…

A. Updates to the journal receivers themselves
B. File operations including when they are opened and closed
C. Record updates
D. Support for commitment control

There are literally thousands of tables in the JD Edwards World application. Fortunately the vast majority of these while not immaterial to an organizations operation, would not warrant database audit monitoring. Every customer is unique and may have a specific audit requirement. However to assist in the selection of files we can consider four types of files.

1. Security files
2. Configuration files
3. Entity files
4. Transactional files

1. Security Files

It is quite apparent why the JDE World security tables should be audited. These will define both access control and what a user can do when they are in an application. Included in the recommended audit file list are the menu tables. These hold masking attributes that can grant or deny access. All too frequently users will create their own instance of menus that call JDE or non JDE applications.

2. Configuration Files

There are many configuration files in JDE. It is these that make the application so flexible and user friendly. The files referred to in the appendix have a particular sensitivity to possible misuse. For example automatic accounting instructions will define the path of automated transactional processing in terms of source and destination accounts.

3. Entity Files

If a fraud were to be perpetrated this would in many cases require the definition of some sort of entity? This might be an account, supplier or fictitious employee.

4. Transactional Files

For whatever reason, be it genuine fraud or human error, the clearest record of what has been done on a system will exist at the transactional level. For that reason the primary transactional files have been included in this section as a recommendation for auditing. While data volumes are unlikely to be an issue for the files in the other areas, the selected audit fields in these tables should be kept under review.

AS/400 Security Architecture

System security is an integrated function of the AS/400 system. It is implemented at the instruction level and controls all AS/400 software functions. Users are identified and authenticated by a single security mechanism, at the system level, for all functions and environments available on an AS/400, including program development and execution, data base applications, office applications, and so forth. All objects on an AS/400 system are under security control, including libraries and files, display stations, operator console functions, programs, menus, and so on.

System Integrity

The integrity of the operating system is an important prerequisite for the implementation of security controls. The AS/400 system has good integrity for several reasons:

- ✓ Precisely controlled storage addressing limits for a user
- ✓ Security implementation at the instruction level
- ✓ A physical keylock controlling the operating system security environment
- ✓ A precisely defined method for providing limited capabilities for users
- ✓ A security system that is an integral part of the total system
- ✓ A communications environment with security features built in at the lowest level
- ✓ Special hardware to validate software pointers
- ✓ Complete auditing capabilities of system and user functions

Since all AS/400 data structures (system and user) are objects, the security system is primarily concerned with protecting objects. All objects have some common structures in their control blocks (invisible to the normal user). This allows a unified approach to security, since all objects interface the same way to the security routines.

AS/400 allows the system administrator to monitor and track system users to ensure they are in compliance with their security policy. It will accomplish this task by providing the ability to create reports on files, libraries, command, user profiles and job descriptions. In addition, it provides reporting on programs that adopt authority, user profiles with access authority, authorization lists, and network values. This reporting will help control system compliance and also identify areas that may require tighter controls.

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

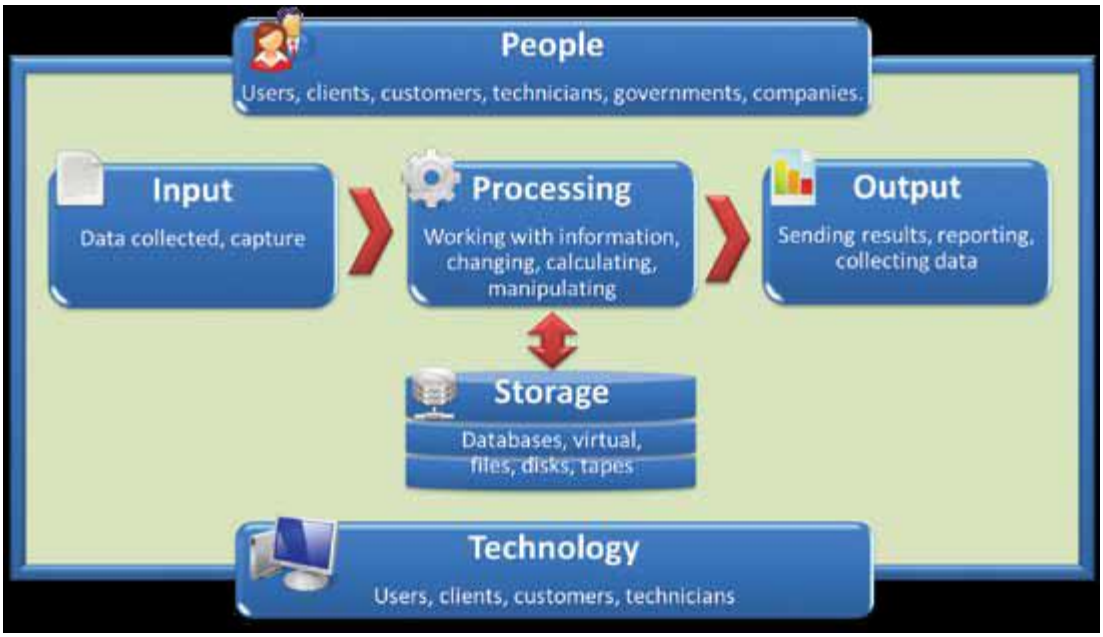
 Master File Maintenance – controls over master file integrity are effective which ensure changes are approved, accurate and complete

 Audit Trail – controls over transaction logs are in place which ensure transaction history is accurate and complete

What we do?

- **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.