The auditor-general of south africa essay sample

Law, Security

The Auditor-General of South Africa has a constitutional mandate and, as the Supreme Audit Institution (SAI) of South Africa, it exists to strengthen our country’s democracy by enabling oversight, accountability and governance in the public sector through auditing, thereby building public confidence.

Foreword

For many organisations, information and the technology that supports it represent their most valuable, but often least understood assets. Successful enterprises recognise the benefits of information technology and use it to drive their stakeholders’ value. These enterprises also understand and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on information technology (IT). The use of technology and IT systems is increasingly embedded into business processes to initiate, authorise, process and manage financial transactions. As a result, weaknesses in the design, implementation or effectiveness of information technology controls this have the potential to not only compromise the integrity and accuracy of financial information, but may impede the efficiency of an entity to achieve its objectives and reporting of business and financial information. Providing access to systems in the face of potential misuse of information is an important issue to be considered by accounting officers, executives and senior management in public sector entities. There are sufficient examples in today’s world to demonstrate that events that can seem unlikely do happen.

Many services delivered by public sector entities are essential to the economic and social well-being of our society − a failure to deliver these could have significant consequences for those concerned and for the nation.

It is part of an entity’s overall approach to corporate governance which should include effective IT governance and risk management, and should be closely aligned to the entity’s incident management, emergency response management and IT disaster recovery. This guide has been prepared based on insights from a number of entities and businesses audited. Establishing, evaluating and monitoring the effectiveness of internal controls over financial information are an important issue which is the responsibility of all public sector entities; and entities’ approaches to these matters are considered by the Auditor-General in determining our audit coverage of entities’ financial statements. While practices described in this publication generally provide guidance to entities, it is important that each entity assesses the extent to which the information provided is relevant, appropriate and cost-effective in light of its own individual circumstances.

Chapter 1 – Introduction

1. Purpose of this guide

This guide is intended to assist the South African government entities in strengthening IT security and controls within their systems. . It aims to guide and assist entities that are looking to: • • • • • identify and assess business impacts and risks that may arise as a result of control weaknesses increase awareness of user account management risks strengthen system security controls and ensure that user access to systems and applications is appropriately restricted and segregated implement better practice procedures to improve delivery of information from IT processes enhance good corporate governance and IT governance practices. government entity has responsibility for the processing and/or system management of financial

transactions on behalf of another government reporting entity. In order to encourage flexible working practices, IT services are introducing and expanding functionality that allows users access to the financial management system via web portals, remote access and virtual networks and, increasingly, synchronised sign-on or single sign-on (SSO) is being adopted by entities to facilitate identity management. As a result, IT system controls such as user account management processes are not only inextricably linked to the overall financial reporting process but form the foundation of an effective system of internal control for financial reporting.

3. Areas covered by this guide

This guide covers those key control objectives that are most likely to be implemented by public sector entities, such as user account management procedures, user registration, modification/changes, user deregistration, review of users' access rights, privilege management, user responsibilities in terms of password usage and equipment, password management and monitoring of access/user activities.

2. Why consider controls?

Increasingly, the reporting process in South African governmental entities is driven by information systems. The use of technology and IT systems is embedded in the business processes to initiate, authorise, process and manage transactions. Today's IT systems have complex interfaces with internal business systems and numerous IT processing or reporting systems and receive or transfer financial information concerning government

payments or grant payments. Government entities are also increasingly implementing ‘ shared services’, whereby one

4. How to read this guide

Each control objective is introduced with a brief narrative description, followed by more detailed procedures and best practices that should be considered to support the achievement of the control objective.

Good practice guide – User account management

Chapter 2 – User account management

1. Background

Organisations should protect their information assets from the risks created by both intentional and unintentional misuse of resources. The implementations of technology are diverse and complex (e. g. platforms, applications, operating systems, databases, email, internet, etc.) and all of them have to be protected from unauthorised use. The risks can, however, be minimised by following the good user account management practices prescribed by the International Organisation for Standardisation, the International Electrotechnical Commission on Information Technology — security techniques — Code of Practice for Information Security Management (ISO/IEC 27002: 2005) and the Information Systems Audit and Control Association’s guideline on access controls (G38). Criteria from these documents as outlined in this brochure could be of great value to organisations when performing self-assessments of access to their systems. therefore be implemented to minimise these risks to a level that is acceptable to the organisation.

Detective controls are also required to secure the process. Proper user account management is one of the processes that can assist in achieving better information security, responsibility and accountability. • The level of access granted to information and systems should be appropriate in terms of the business purpose and should be consistent with an organisational security policy, e. g. it should not compromise segregation of duties (duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation’s assets). A written statement should be issued to users explaining their access rights. Users should sign statements indicating that they understand the conditions under which access is granted. Unique user identifications (IDs) should be created that identify users and link their actions to their IDs. Redundant user IDs should not be issued to other users.

3. User account management procedures

These procedures should cover all stages in the life cycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access to information systems and services. All procedures should be documented and formally approved (signed and communicated). It should also be ensured that access control responsibilities, e. g. access request, access authorisation and access administration and monitoring, are segregated throughout the process.

5. Modification/changes

Changes in user status include changes of job function, roles, responsibilities and transfers within the organisation. A procedure should be established to

manage these changes in user status and should include, inter alia, the following: • Changes should be communicated to information owners, users, superusers, supervisors or any person/department responsible for defining, granting, changing or revoking access privileges. The access rights of users who have changed job function, roles, responsibilities, etc. should immediately be removed or blocked. Procedures as for the registration of users should be followed when the status of a user changes.

4. User registration

A formal user registration procedure for granting access to information systems and services should be in place. This procedure should ensure the following, inter alia: • • • A formally documented access request should be completed and be approved by the user’s supervisor. The access request form should make provision for adequate details regarding the user, supervisor, type of access, approvals, etc. to be provided. Approval from the business/system owner should be obtained before access is granted to business information resources.

2. Introduction

Poor access control practices can lead to unauthorised disclosure of confidential information (confidentiality), unauthorised changes to data (integrity) or loss of continuity of business (availability). The consequences of not having appropriate access controls in place should be considered in terms of the value of the asset to the organisation from both a quantitative and a qualitative perspective, e. g. reputation impact, customer/public perceptions, regulatory effect and financial effect. Preventive controls should

6. User deregistration

The access rights of users who have left the organisation should immediately be removed.

of system administration privileges can be a major contributing factor in failures or breaches of systems. A formal authorisation process should be used to control the allocation of privileges in multi-user systems that require protection against unauthorised access. The following steps should be considered: • The access privileges associated with each system product, e. g. operating system, database management system and each application, as well as the users to which they need to be allocated, should be identified. Privileges should be allocated to users on a needto-use basis and on an event-by-event basis, i. e. the minimum required for their functional role and only when needed. An authorisation process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorisation process is complete. Privileges should be assigned to a different user ID than that used for normal business activities. Changes to privileged accounts should be logged for periodic review.

9. 1 Password usage

Passwords are a basic control in verifying a user’s identity before access is granted to an information system or a service according to the user’s authorisations. Each employee is responsible for all the actions performed with his/her password, even if it is demonstrated that an action was carried out by another individual using the user’s password. Users should therefore follow good security practices in the selection and use of passwords and the

following should be kept in mind: • • • • Keep passwords confidential. Avoid keeping a record of passwords, e. g. hard copy or electronic file. Change passwords whenever there is any indication of possible system or password compromise. Compose passwords that are: o easy to remember o o of sufficient minimum length, e. g. six characters not based on anything somebody else could easily guess or obtain using person-related information, e. g. names, telephone numbers, dates of birth, etc. not vulnerable to dictionary attacks (i. e. do not consist of words included in dictionaries) free of consecutive, identical, all-numeric or all-alphabetic characters.

7. Review of user access rights

The review of users' access rights is necessary to maintain effective control over access to data and information services. Users' access rights should therefore be reviewed as follows: • • At regular intervals, e. g. every six months After any changes such as: o promotion o o • • • • demotion termination of employment

When moving from one section/division to another within the same organisation Authorisations for special privileged access rights should be reviewed at more frequent intervals, e. g. every three months. Privilege allocations should also be reviewed at more frequent intervals to ensure that no unauthorised privileges have been obtained. All changes to privileged accounts should be logged for periodic review.

9. User responsibilities

The cooperation of authorised users is essential for effective security. Users should be made aware of their responsibilities for maintaining effective

access controls, particularly regarding the use of passwords and the security of user equipment.

8. Privilege management

The allocation and use of privileges should be restricted and controlled.

Inadequate control

Change passwords at regular intervals or based on the number of times access has been obtained. The passwords for privileged accounts should, however, be changed more frequently than normal passwords. Avoid the reuse or cycling of old passwords.

Change temporary passwords at first logon. Never share individual user passwords among users.

10. User password management

The allocation of passwords should be controlled through a formal management process and this process should include the following requirements as a minimum: • Users should be required to sign an undertaking to keep personal passwords confidential. This signed statement could also be included in the terms and conditions of employment. If users are required to maintain their own passwords, they should be provided with a secure initial password, which they should be required to change immediately at first logon. Procedures should be established to verify the identity of a user prior to providing the user with a new, replacement or temporary password. A secure procedure should be followed when granting users temporary passwords and the use of unprotected (clear text)

electronic mail messages should be avoided. Temporary passwords should be unique and should conform to password standards. Users should acknowledge receipt of passwords. Passwords should never be stored on computer systems in an unprotected form. Default vendor passwords should be replaced as soon as the installation of systems or software has been completed.

11. Monitoring of access/user activities

A set of controls should be defined for controlling and monitoring user access to and activities on systems. The following should, inter alia, be considered:

• • Repeated failed login attempts should be identified and investigated. Any blocked or suspended user ID (three or more consecutives failed attempts) should be investigated to verify that the user is the authorised owner of the user ID and not an unauthorised person trying to discover passwords. Inactive users should be monitored and corrective action should be taken after a predefined period of inactivity, e. g. users that have been inactive for 60 days should be blocked. Activity carried out by default users (e. g. guest, administrator, owner and root) should be monitored on a daily basis.

Access to critical accounts, log files, data files and databases should be monitored. Periodically, logs should be reviewed to monitor the activities of privileged users and failed access attempts. The organisation should be prepared to react appropriately should a breach of access such as an unauthorised intrusion be detected. Periodically, the organisation should check for and remove or block redundant user IDs and accounts. The activities of the privileged or superuser login account should be

closelymonitored and reviewed by senior computer security management. Users’ passwords should be reviewed to ensure that an appropriate level of complexity is maintained.

9. 2 Unattended user equipment

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities in regard to the implementation of such protection. Users should be advised to, inter alia: • terminate active sessions when finished, unless such sessions can be secured by an appropriate locking mechanism, e. g. a password-protected screen saver log computers off at the end of a session (i. e. it is not sufficient to merely switch off the PC screen or terminal) secure computers from unauthorised use by means of a key lock or an equivalent control, e. g. password access, when not in use.