ACS 1803 SUPPLEMENTARY NOTES – Auditing and Controls

More on Controls

ACCESS CONTROLS

Need to know : It is based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their job duties.

In the field of information technology, **access control** is the selective restriction of access

There are physical access controls and electronic controls.

Access controls can be categorized in two ways: physical access controls and electronic access controls. Physical access controls are used mainly to ensure that an organization's computer resources and facilities are safeguarded against physical abuse, damage and destruction. Electronic access controls, on the other hand, are mainly used to safeguard the integrity and confidentiality of the information in the system. Physical and electronic access controls must generally be used in combination to achieve a level of security considered appropriate for the enterprise.

The basic objectives of any type of access control mechanism or device are to deter an intruder from wanting to access the computer system by making unauthorized access very difficult, yet at the same time permit authorized users to easily access the system.

Access Control Practices *MC

- Deny access to systems by undefined users or anonymous accounts.
- Limit and monitor the usage of administrator and other powerful accounts.
- Suspend or delay access capability after a specific number of unsuccessful logon attempts.
- Remove obsolete user accounts as soon as the user leaves the company.
- Suspend inactive accounts after 30 to 60 days.
- Enforce strict access criteria.
- Enforce the need-to-know practice.
- Disable unneeded system features, services, and ports.
- Replace default password settings on accounts.
- Limit and monitor global access rules.
- Ensure that logon IDs are nondescriptive of job function.
- Enforce password rotation.
- Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
- Audit system and user events and actions and review reports periodically.
- Protect audit logs.

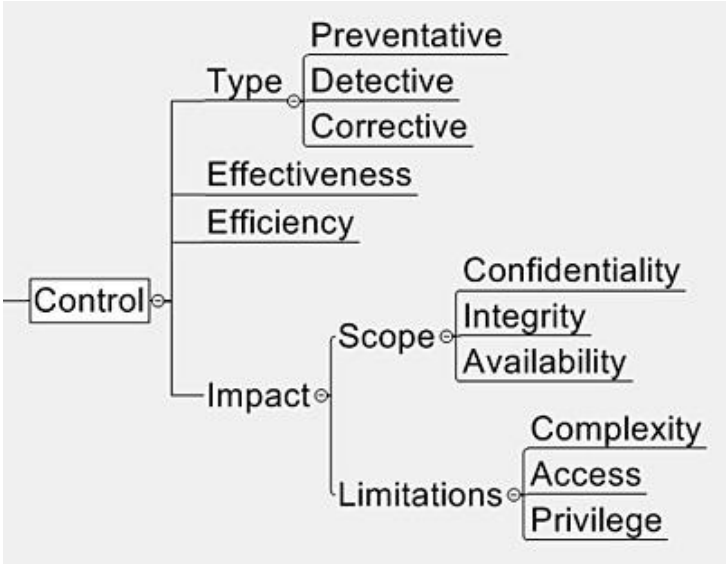
ERROR LOGS: To ensure the completeness of error correction, all errors should be logged in manual or computerized logs. Responsibilities for error correction should be clearly defined. The error logs should be monitored to ensure that the errors are corrected on a timely basis. Error statistics should be kept as a way of focusing in on recurring error conditions to help focus attention on documents or transaction screen layouts which may need redesign, employees that may need further training, manuals that may need to be revised and improved, or programs that may need to be modified.

Application System Controls (e.g., for AIS component systems)

****L Question: Explain clearly three types of application controls and give one example in each type.**

Types of Controls

A Vulnerability is a defect in a process, system, application or other asset that creates the potential for loss or harm. Vulnerabilities are measured primarily through the identification of control deficiencies (defects or weaknesses) to determine a system's or process' propensity for failure.



In terms of taxonomy, there are three, commonly accepted forms of Controls:

1. **Administrative** - These are the laws, regulations, policies, practices and guidelines that govern the overall requirements and controls for an Information Security or other operational risk program. For example, a law or regulation may require merchants and financial institutions to protect and implement controls for customer account data to prevent identity theft. The business, in order to comply with the law or regulation, may adopt policies and procedures laying out the internal requirements for protecting this data, which requirements are a form of control.
2. **Logical** - These are the virtual, application and technical controls (systems and software), such as firewalls, anti virus software, encryption and maker/checker application routines. Logical tools used for identification, authentication, authorization, and accountability in computer information systems. They are components that enforce access control measures for systems, programs, processes, and information. Logical access controls can be embedded within operating systems, applications, add-on security packages, or database and telecommunication management systems.
3. **Physical** - Whereas a firewall provides a "logical" key to obtain access to a network, a "physical" key to a door can be used to gain access to an office space or storage room. Other examples of physical controls are video surveillance systems, gates and barricades, the use of guards or other personnel to govern access to an office, and remote backup facilities.

All three of these elements are critical to the creation of an effective control environment. However, these elements do not provide clear guidance on measuring the degree to which the controls mitigate the risk. Instead, the Simple Risk Model utilizes an alternative set of elements that provide a better means of weighting the level of mitigation:

1. **Preventive** - These are controls that prevent the loss or harm from occurring. For example, a control that enforces segregation of responsibilities (one person can submit a payment request, but a second person must authorize it), minimizes the chance an employee can issue fraudulent payments.

   The use of **authorization tables** within the authorization program will provide several additional levels of control. For example, such tables may be used to match up a particular user with the:
   - Specific terminals s/he is permitted to use;
   - Specific data files s/he is permitted to access;
   - Specific programs s/he is permitted to request;
   - Specific records or even fields within the records that s/he is permitted to change;
   - Specific transactions that s/he is permitted to enter; and even,
   - Time(s) of day that each of the above may occur.

   Access to such tables should itself be restricted to a very select number of authorized personnel.

2. **Detective** - These controls monitor activity to identify instances where practices or procedures were not followed. For example, a business might reconcile the general ledger or review payment request audit logs to identify fraudulent payments.

   Monitor and investigate any lack of activity of regular customers, personnel and suppliers.

   The lack of activity of regular customers, personnel, and suppliers may indicate that transactions have been omitted or lost subsequent to initiation. For example, an analysis of regular customers without transactions during a period may point out shipments that were made but were not billed.

   Prepare budgets and financial forecasts and investigate variances between these and the entity's actual performance.

   Differences between budget and actual amounts may be caused by errors or omissions in transaction processing.

   Where practical, establish procedures for verification of output by users.

   Design programmed reasonableness tests into the information system.

   Print out semi-permanent data, or a sample thereof, for review by knowledgeable users for obvious errors.

   It is generally desirable to periodically print out critical information for visual review by the source department or by internal audit. For example, the payroll master file might be periodically listed and agreed to current personnel records to ensure the accuracy and validity of employee names and pay rates.

3. **Corrective** - Corrective controls restore the system or process back to the state prior to a harmful event. For example, a business may implement a full restoration of a system from backup tapes after evidence is found that someone has improperly altered the payment data.

   Of the three types of controls, preventative controls are clearly the best, since they minimize the possibility of loss by preventing the event from occurring. Corrective controls are next in line, since they minimize the impact of the loss by restoring the system to the point before the event.

   However, the restoration procedure may result in some degree of loss, since the restoration procedure may lead to the unavailability of systems and applications along with possible lost productivity, customer dissatisfaction, etc. The least effective form of control, but the one most frequently used, is detective controls - identifying events after they have happened. Depending on how soon the detective control is invoked after an event, a business may uncover a loss long after there is any opportunity to limit the amount of damages. In the Proof-of-Concept application, the Control is weighted by whether it is a preventative, detective or corrective control.

   Computer edits and other programmed controls generally result in either the rejection of transactions from further computer processing, or the acceptance but flagging of transactions for review. It is essential that such errors and exceptions be followed up and corrections made where necessary. Failure to do so will result in either incomplete or inaccurate processing.

   Use error logs.

   Monitor and investigate any lack of activity of regular customers, personnel and suppliers.

   The lack of activity of regular customers, personnel, and suppliers may indicate that transactions have been omitted or lost subsequent to initiation. For example, an analysis of regular customers without transactions during a period may point out shipments that were made but were not billed.

   Prepare budgets and financial forecasts and
   investigate variances between these and the entity's actual performance.

   Differences between budget and actual amounts may be caused by errors or omissions in transaction processing.

   Where practical, establish procedures for verification of output by users.

   Design programmed reasonableness tests into the information system.

   Print out semi-permanent data, or a sample thereof, for review by knowledgeable users for obvious errors.

   It is generally desirable to periodically print out critical information for visual review by the source department or by internal audit. For example, the payroll master file might be periodically listed and agreed to current personnel records to ensure the accuracy and validity of employee names and pay rates.

(credit: CICA IT Control Guidelines)

TRUST SERVICES

What is WebTrust? *L

WebTrust is a seal awarded to web sites that consistently adhere to certain business standards established by the Canadian Institute of Chartered Accountants (CICA.ca) and the American Institute of Chartered Public Accountants (AICPA). Now globally recognized, these standards can be in the areas of privacy, security, business practices/transaction integrity, availability, confidentiality or non-repudiation.

The need for Trust Services, such as WebTrust, have grown considerably in recent years, due in large part to the advent and growth of e-commerce and the overall e-business environment, which results in **tremendous amounts of sensitive and confidential data traversing from entity to entity, often involving financial related information. In short, we live in a digital world where information is transparent, readily available, and can be accessed anytime by almost anyone, anywhere. The need to protect e-commerce systems and other supporting I.T. systems and platforms is vitally important, now more than ever.**

Why was WebTrust developed? *MC

WebTrust was developed to addresses consumer and business concerns over privacy and security. WebTrust has evolved to also address the inability of businesses and consumers **to confirm the legitimacy of companies offering goods and services over the web**.

Backed by the CICA and AICPA, WebTrust is an Internet seal that can give web-goers true confidence that certain businesses can be trusted with consumers' (and business') most important asset and prized possession: their **private information**. What makes WebTrust different from all other Internet seals? Independent verification is the key to WebTrust.

WebTrust is a seal administered by a third-party. That means when you see a WebTrust Seal on a web site, the owners had to meet standards set by the professional accounting bodies of Canada and the United States (CICA & AICPA). And the site is audited for WebTrust compliancy at least every 6 months.

The owner of a web site who has been granted a WebTrust Seal believes that privacy (or security) is so important to their clients and business partners, that they have:

... hired specially trained and licensed WebTrust auditors to review their online procedures (particularly in the area of privacy)

... maintained the highest business standards found on the Internet

... agreed to have their online procedures regularly audited to make sure the standards are maintained.

WebTrust Seals can be awarded to web sites if they've consistently maintained those high standards in the areas of security, business practices/transaction integrity, availability, confidentiality and non-repudiation.

Is there more than one WebTrust Seal to choose from? *X

There are six WebTrust Seals. To be granted any WebTrust Seal, a firm must demonstrate that it has consistently maintained high standards, set by the CICA and AICPA. The six areas are:

... **Privacy -** adhering to the strictest rules for collecting, storing and using client/customer information. Benefit to you: demonstrates that your business is trustworthy.

... **Security -** following the most appropriate and current safety measures, technologies and procedures. Benefit to you: gives online/offline customers peace of mind.

... **Business Practices/Transaction Integrity -** reducing fears that information can be stolen during an online transaction, and that the transaction will be completed successfully. Benefit to you: reduces your customers' fears/apprehension of buying online.

... **Availability -** maintaining the service levels outlined in your agreements with customers and clients. Benefit to you: strengthens your attractiveness as an Application Service Provider (ASP).

... **Confidentiality -** demonstrating the ability to protect business-to-business information. Benefit to you: gives your business customers confidence in your ability to exchange information online.

... **Non-Repudiation -** confirming customers' identity and ability to pay for their online purchases. Benefit to you: protects your revenues.

Trust Services Principles *MC

The following principles and related criteria have been developed by the AICPA and the Canadian Institute of Chartered Accountants (CICA) and are the foundation of the Trust Services Framework:

1. **Security**: The system is protected against unauthorized access (both physical and logical).
2. Availability: The system is available for operation and use as committed or agreed.
3. **Processing integrity**: System processing is complete, accurate, timely, and authorized.
4. Confidentiality: Information designated as confidential is protected as committed or agreed.
5. **Privacy**: Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CICA.

***MC : Canada's federal Privacy Law** applicable to the private sector is formally referred to as Personal Information Protection and Electronic Documents Act(PIPEDA). The purpose of the act is to establish rules to govern the collection, use and disclosure of personal information by commercial organizations. The organization is allowed to collect, disclose and use the amount of information for the purposes that a reasonable person would consider appropriate in the circumstance.[27]
