

Project SL. NO. (7): Based on the Frameworks for Projects at SL. Nos. (4-6), discuss the inadequacy of application controls to ensure Information Integrity.

Framework:

Application Controls and Beyond

Traditionally, errors in information system (IS) and resulting integrity implications have been addressed as if they were preventable or correctable by building controls within application system. With time there have been efforts to put in greater inputs right at the system analysis and design stage, hoping that would ensure Information Integrity.

However, as mentioned in the introduction, reality is different. Main reason for this is ironically the inadequacy of controls designed to meet lapses in integrity.

(a) At different IS stages

(a – 1) Data collection procedures and codes

For example, to avoid lapses in integrity at the stage of operating data collection procedures and codes, controls implemented are: upgradation of manual testing, improved updating procedures, location control of manuals, manual preparation by technical writers, testing of documentation by users, user documentation standards, etc. Further, particularly in the user environment, controls visualized are : improved documentation distribution, policies to control duplicating and copying manuals, documentation of frequency of errors and source, performance checks of manual users.

However, with shared data environments, with user community spanning entire enterprise and with human element of carelessness, it is extremely difficult to avoid situations like manual unavailable when needed, use of unauthorized manual, user inability to understand manual language, resulting in the use of wrong procedure or code and, therefore, in inaccurate and insecure data in spite of controls.

(a – 2) Form filling stage

At the form filling stage, to avoid errors due to ambiguous directions and poor format, system designers implement controls in terms of form preparation by analysts experienced in form design, upgradation of testing (including testing by user groups), etc. Further, to avoid errors due to substitute or unauthorized person filling out forms and to avoid errors due to poor motivation and carelessness, controls are exercised by having distribution and collection controls, requiring identification of user, giving instructions emphasizing positive benefits of correct data and negative effect of wrong information, use of turnaround documents, etc.

However, situations of poor motivation, carelessness and substitute or unauthorized persons filling out forms continue, resulting in incorrect filling of forms.

(a – 3) Data collection stage

At data collection stage, controls implemented are : glance-check data, use of header

cards, improved employee training, use of turnaround documents, check digits, upgrading form control, upgrading code control, use of conventions for writing numbers and letters, requiring type input, use of boxed spaces on forms, logging of all data, separation of duties, careful selection of people, audit procedures, etc.

These controls may result in eliminating errors due to poorly designed forms, codes and poor handwriting, but errors caused due to carelessness are very difficult to eliminate completely.

(a – 4) Data preparation stage

Coming to the data preparation stage, controls exercised are : upgraded procedures manual including visual aids, proper maintenance, verification of keypunching by a second operator, use of check digits, glance check, upgraded training and employee selection, upgraded procedure testing, log data, etc.

However, all these controls are not sufficient to eliminate error implications of carelessness in data preparation. Further, it is also extremely difficult to ensure controls like employee selection and training for foolproof results.

(a-5) Machine operation stage

At the machine operation stage, solutions or controls implemented are : upgraded personnel selection, training and procedure testing, upgraded maintenance, testing upgraded, backup equipment, shutdown devices, intrusion detectors, patrol, control of physical access, control access to files, at least two people on duty, steel or steel mesh on windows and doors, remove conflict of interest, vary work schedules, strict supervision, establish documentation procedures (logging, checking, record totals), etc.

Even then, errors caused particularly due to human behavior like carelessness of operators, sabotage, desire for personal gain, documents lost or misrouted are difficult to eliminate. Once again, it is difficult to have controls like upgraded personnel selection or training that are foolproof.

(a-6) Communication channels at pre and post processing stages

As regards to the communication channels, both at pre-processing and post-processing stages, controls implemented are access controls and the use of cryptography protocols. Parity checks facilitate error detection. A bit of data is added to each set of bits representing a character so that total number of 1 bits is odd (for an odd parity check) or even (even parity check). Upon receipt of the transmission, the bits are added and compared to the parity rule. When an error is detected, a signal is sent for retransmission of data. Checking for the use of a prescribed pattern of ones and zeroes to represent characters is another method of tracing error.

Access control is also a method guarding a system from unauthorized use (security requirement). With on-line systems using telecommunications, security is a greater problem, for stringent access control to terminals (like badge systems, locked doors, a buffer zone, or entry guards) may not exist at remote sites. The computer itself must, therefore, determine the legitimacy of users by having three dimensions: identification

(say through passwords) and authentication and authorization (through a data directory security matrix).

Computer processing is today closely linked with telecommunications, allowing the transference of computer data between remote points. Protecting the confidentiality of this data at the terminal when transmission is initiated or received or from intrusion during transmission itself, has required the development of sophisticated controls.

A "handshake", a pre-determinable signal which the computer must recognize before initiating transmission, can control access to the system. Protocols, conventions, and procedures for user identification and dialogue termination help maintain confidentiality of data.

During transmission, messages are vulnerable to wiretapping, the electromagnetic pickup of messages of communication lines. This may be eavesdropping, passive listening, or active wiretapping, involving alteration of data, such as piggybacking (the selective interception, modification, or substitution of messages). It is such message interceptions that are prevented/controlled by encoding or encrypting data.

In spite of all these communication controls, errors caused by failure of data communication software, channel noise, and unpredictability of data communication network due to its size and complexity, not to speak of adverse influence of people and weather, are difficult to eliminate.

Controls during machine operation at pre-processing stage and their inadequacy are same as that for machine operation following the data preparation stage discussed earlier.

(a-7) Data files

Coming to data files, controls considered are controlled humidity storage, "clean room" conditions, special cabinets, periodic cleaning, centralized storage under librarian, upgrading of storage procedures, backup data and controlled access to files. However, these controls can not completely remove causes of theft, fraud or sabotage which stem from human behavior.

(a-8) Systems and Application Software

As regards to the systems and application software, they are characterized by controls such as : upgrade training of programmers, establish standard programming procedures, testing upgraded : desk check, manual check, compare historical results, cross check totals, establish and enforce documentation standards, check programs against original version periodically, team program auditing, etc.

However, all these controls still do not ensure removal of all errors, particularly those caused during programming and those due to poor documentation and lax security.

(a-9) Processing stage

At the processing stage, controls implemented are through validation tests which detect

many errors introduced at form filling stage, data collection stage and data preparation stage. These tests include checks for completeness, format, range, reasonableness, consistency, sequence, transaction count, and recalculation of check digits.

These validation tests determined by users, should be specified with care for under specification leads to undetected errors, causing information system to produce unreliable information, where as over specification adds unnecessarily to processing costs. Further, as observed by Svanks in her significant research work entitled "Integrity Analysis : A Methodology for EDP Audit and Data Quality Assurance", this validation is normally according to stated specifications by the use of a validation table. This table encodes the requirements each data element must satisfy before it can be declared acceptable. For example, an element may be specified to fall between a permissible minimum and maximum value. However such validation does not exploit element relationships, and hence does not ensure data integrity. In other words, because data is validated largely at element level, real data bases contain inconsistencies.

Other processing controls are upgrading training of personnel, log jobs, use standard labels for all files, programs to automatically upgrade updated data, upgrade planning and inventory control of necessary supplies.

However, all these controls at processing stage cannot remove errors that are caused by carelessness.

(a-10) Output stage

Finally, at the output stage, controls implemented are: audits, validation programs, interfile comparison, defer large volume printing until proof data checked, sample check of output with corresponding input, sight check, check page counts, check control totals for each process of report etc.

And, yet, these controls can not always eliminate, all operation or processing errors.

(b) Human error: a significant integrity problem

As one critically considers the above discussion amongst others, factors of carelessness, poor motivation, and other actions of people emerge as most significant factors contributing to errors in information system and, thereby, lapses in integrity. According to a study performed by the Executive Information Network, 55% of the respondents involved in a survey considered human error as the most important integrity threat. Ironically, human error can also be one of the most serious problems causing system interruptions.

While the frequency of human error and the opportunity for human error are important considerations, the magnitude of the loss due to human error is also a major concern. Contrary to the general opinion of many information system practitioners, human error is not always a low-consequence threat. In fact, in terms of money lost, human error is the largest single cause of economic and productivity loss in the information system integrity arena. As an evidence of this, consider a study reported in Computerworld, which attributes 52% of corporate information damage to human error. Single-incident losses can also be significant.

Rapidly evolving technologies producing distributed information networks and shared data environments that are commonplace today pose yet another issue. Once an error occurs it can be considered an "inherited error" if it is passed along to another computer, network, database, file, or the like. Inherited errors occur when an error is propagated beyond the system in which it originated. For example, if a personal computer on a local area network is used to prepare a report - and erroneous data is incorporated into that report - when the report is submitted to another computer system, an error is inherited.

Various controls that are considered and implemented can not remove these human error possibilities, as can be seen from the feedback on error occurrences and their consequences as available from the field.

Inadequacy of controls

Information user's concern for integrity of information obtained from information system has undergone an almost cyclic transformation in the past few decades. Centrally located, batch-oriented systems of 30 years ago suffered from the inherent unreliability of their many discrete components, which made system failure frequent and maintenance complex and time-consuming. Consequently, much effort and ingenuity was expended in those days in devising fault detection and automatic correction techniques to defend computer against the effects of hardware failure to which it was prone.

Thus in the early days of computing, numerous studies were carried out on errors in data transcription. Experiments were devised where groups of people were assigned tasks of encoding, writing, copying, keying, and reading large volumes of data and results of these experiments were then analyzed to determine the frequency of various types of errors. Many commonly used data validation techniques and controls, including handwriting and forms design standards evolved on the basis of these findings.

Later, however, with the advances in manufacturing technology exemplified by medium scale and large scale integration, these problems were alleviated considerably, both by improved component reliability and an increase in density of logic gates per replaceable pack, which reduced the difficulty of maintenance. Concern over hardware unreliability and consequent information error therefore abated.

However, as computer systems become increasingly networked, as applications increasingly share data with one another, and as databases become increasingly distributed, the risk of data/information error - including risk of inherited error increases, which amounts to the issue of data/information pollution.

Factors external to Application Controls

As discussed through this Section, these errors are caused by factors not amenable to controls including application controls conceived at system design stage itself. Of course, literature reports research efforts in terms of identifying foolproof information requirements, but design experience shows this is something not easy to achieve.

This is because, due to factors detailed here, computerized information systems invariably have errors that are made but not corrected by the controls incorporated at system design stage. As can be seen, these factors, invariably have their presence mainly

through the system environment which is external to computing (and hence the application) system and overlaps the user environment, though together they (the computing system and its external environment) constitute the Information System Model. In spite of application controls, it is these external factors that then make information systems give rise to information which is inaccurate, inconsistent and unreliable.

These external factors could be categorized into five major categories; namely, Change, Complexity, Communication, Conversion, Corruption.

Change

Change may occur either in the content or in configuration of the system environment, resulting in a possibility of error introduction in the information system. Every hardware change, software release, and organizational change will come under this category, offering cause for error and, therefore, for a possibility of an inaccurate, inconsistent or unreliable information.

Complexity

Whenever one introduces complexity, there is a possibility of error introduction in the information system. Every new component, be it a program, database or network, adds new interfaces increasing the possibility of error introduction.

Communication

Communication stands for movement of data/information within or across enterprises and it also provides a chance for error introduction.

Conversion

Conversion, in this context, refers to the consolidation, decomposition or transformation of data. Whenever one converts data from one form to another, there exists a possibility of error introduction, resulting in information which may not be accurate.

Corruption

Finally, category corruption pertains to human behavior (poor motivation, desire for personal gain, carelessness, actions of people, to factors leading to inherited errors polluting the information systems, and to unpredictability (noise) of any kind leading to introduction of errors in computerized information systems.

Whether, in addition to controls discussed above, computerized information systems also incorporate human engineering design criteria at the system design stage itself or hardware and software vendors further incorporate error-checking filters into their products, it is these external error factors that then have to be addressed, if one were to resolve the question of errors in Information System Models so as to obtain Information which is Accurate, Consistent and Reliable.