Good case study on types of input control

Technology, Internet

Input Controls:

Input Controls:

Introduction and Functions of Input Controls:

Data input controls refer to application specific user interface components, data and/or transactions used to ensure that data in a computer system is accurate, complete and is entered in a timely manner. Input controls are mainly used when entering data into a computer application or when converting data from the source format into computer data. Data is usually entered into computer applications and systems through manual online input, or through the use of automatic processing. The main function of input control is to ensure data integrity in business applications regardless of whether data is entered into the system directly, remotely by a partner or through a web interface (AMAS, 2012). For quality assurance purposes, input controls are used to ensure the accuracy of data input and the optimal use of computerized validation, error handling and editing procedures. This also ensures that integrity errors are corrected and that data is accurately and timely resubmitted (Bellino et al., 2007).

Additional input control functions and components include whether the controls are preventive or defective, and they operate within applications based on configurable or programmed system logic. Preventive input controls are used to prevent errors from occurring in applications and example is a data input validation routine. The input validation routine checks to ensure that data is consistent with the associated program logic and that the system only saves correct data. In this case, invalid or incorrect

data is rejected immediately during data entry and is only accepted after successful corrections have been made (Bellino et al., 2007).

Detective controls identify errors on the basis of a predefined program logic. A good example of a detective input control is one that identifies both favorable and unfavorable variations between the price in a purchase order and invoice price. Detective controls are usually used to support manual controls used in the environment. In fact, the results of such controls can be used to support monitoring tools. For instance, the detective tool previously mentioned can identify variations in the purchase price and to list the exceptions in a log or report. When the exceptions are reviewed by management, then they input control can be considered as a monitoring tool (Bellino et al., 2007).

There are various types on input controls that include cross-checks, limit and reasonableness checks, format and required field checks, sequence, range and digit checks, and validations.

Reasonableness checks are used to ensure that the input data matches the predetermined reasonable limits and occurrence rates. Such checks re mainly used for financial values to ensure they do not exceed certain values or when entering dates e. g. one cannot enter the date of birth as a future date. Format checks are used to ensure the correct syntaxes during data entry e. g. date and time formats while required field checks are used to standardize input and ensure that certain input field are filled before submitting any data. Required field checks are used with values such as email, identification numbers that are needed. Sequence checks are used to check for missing data items while range checks are used to check data

ranges to ensure data is entered into the correct rows and columns in database tables. For example, to ensure that data entered does not exceed the number of columns in a table. Digit checks controls ensure that only numerical values are entered especially when such data is required for calculations (Bellino et al., 2007).

Cross check input controls check for correct data reentry and whether the data agrees with a predetermined set of criteria. Cross check input controls are mostly used for policies that are only valid with some premium table codes. Finally, validation checks are programmed to check the validity of data entered and whether it meets a certain predefined criterion. Examples of validation checks include drop-down menus containing valid items from a stored data table (Bellino et al., 2007).

Data integrity errors that would occur if input controls were not in place:

In the case of reasonableness and limit checks, possible data integrity errors that could occur if the controls were not in place are unreasonable financial values extending beyond or below the set limits. Other integrity errors include possible entry of unreasonable dates such as the date of birth set in the future. Possible data integrity errors that would occur in the absence of format checking input controls include lack of standard data entry formats such as for format sensitive data such as dates, time and email addresses. In the case of required fields, errors include missing data that would read to incomplete records lacking critical data.

If sequence and range check controls are not implemented, the resultant integrity errors include missing data records and wrongly inserted database

records. As for digit check controls, errors would occur due to entry of text and other characters that cannot be calculated.

Finally, if cross check and validation input controls are not implemented, a variety of errors are expected. These errors include missing data records, wrong data formats and values such as emails and dates, incorrect details, and inconsistent data records in the case of crosschecks.

Advantages and Disadvantages of Restricting User Interfaces:

Restricted user interfaces also known as constrained user interfaces are usually designed on the underlying principle that users are only allowed to access system functions for which they are authorized. Restricted user interfaces thus restrict users from accessing functions, information and other specified system resources by denying them the ability to request the use of these resources. User interfaces can be restrained using menus, database views and physical restrictions on the user interface (Guttman & Roback, 1995).

The advantages of restricted user interfaces include access control whereby system administrators can control what the user can access in the system. Menus give a predefined list of options thus only allowing the user to access the given functions. This helps improve system security, makes the system easier to use and eliminates data integrity errors. The main disadvantages when menus are used to restrict user interfaces include lack of flexibility in editing menus especially when system modifications are required, or when users require temporary access to some unauthorized functions (Guttman & Roback, 1995).

Database views are used as mechanisms to restrict user interfaces regarding access to data contained in databases. In this case, users can easily be allowed to access database records but particular users may not require access to all data. Database views are thus highly flexible and can be used to enforce complex data access needs often required in database scenarios. For example, when the receptionist is granted user access to the client database, a database view can be used to grant a user access to the records based on the contact details table only. In this case, other client data such as financial information remains hidden from that particular class of user. Another advantage is the ability to grant data modification rights to certain users thus ensuring accountability and data integrity. The disadvantages of database views include technical complexities that arise when defining access permissions to users while still ensuring accountability and data integrity (Guttman & Roback, 1995).

The third method of user interface restriction is using physically restricted user interfaces. In this case, the system user interface only provides a select number of options and a limited number of physical buttons. Physically restrained user interfaces usually lack a full keyboard e. g. An Automated Teller Machine (ATM) machine. Physically restrained user interfaces thus ensure that users cannot escape to a different system interface. The restriction helps ensure system security by preventing users from bypassing the logical access controls set by system administrators. The main drawback of physical user interface restriction is the cost associated with building such a system and tailoring it to an organization’s needs (Guttman & Roback, 1995).

A graphical representation of a Web-based input for making a hotel reservation using Microsoft PowerPoint:

References:

AMAS,. (2012). Application Self Evaluation. Audit and Management Advisory Services (AMAS). Retrieved 6 November 2014, from http://amas. syr. edu/AMAS/display. cfm? content_ID=%23((%25!%0A

Bellino, C., Wells, J., Hunt, S., & Enterprise Controls Consulting LP,. (2007). Auditing Application Controls (1st ed., pp. 2, 18). Altamonte Springs, FLORIDA, USA: Institute of Internal Auditors. Retrieved from http://faculty. usfsp. edu/gkearns/Articles_Fraud/Auditing_Application_Controls. pdf

Guttman, B., & Roback, E. (1995). AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK (pp. 200-201). WASHINGTON DC: National Institute of Standards and Technology (NIST) Special Publication 800-12.