Creating a flowchart design for the validation check process - lab report example...

Finance

Creating a Flowchart Design for the Validation Check Process

INPUT VALIDATION CHECKS ID] s INPUT VALIDATION CHECKS In the process of Taibert Corporation deploying the expertise of a programmer to develop an online data entry system that minimizes the level of knowledge required by the operator, it is important for the programmer to ensure that the data received and processed by the application is sufficiently validated (Nick, 2003). This is a step to bar common vulnerability that may be exploited by malicious users. This includes understanding the type of data the system should recognize and accept; its syntax, minimum and maximum length of each entry. This kind of specifications validates each input (Nick, 2003).

Input validation check may either use blacklisting approach or white-listing approach. White-listing allows programmer to define the data that should be accepted in an entry while blacklisting does the opposite. That is, a blacklist approach defines a set of ‘ known bad inputs’ that should not be accepted as an input whereas a white-list defines a set of known good inputs.

Using the two approaches, one of the input checks may be application of a white-list. The auditor may consider checking the accepted data types in each entry. For example in the access routine number to payroll by the operator, one may specify that the input must consider of letters, special characters such as dollar sign and numbers. Since it acts like a password, the combination ensures security when it comes to accessibility (Nick, 2003).

Additionally, employees’ number inputs may be restricted to letters and numbers only e. g kw997836.

Besides, another input validation check to consider is canonicalization of all

inputs. This involves reducing data received to its simplest form. Simplifying one input may facilitate bypassing of validation functions. Thus canonicalization ensures that any malicious user do not bypass the validation function (Nick, 2003). Last but not least, one may consider creating checks for the system content. Check for content specifies the maximum and minimum lengths of entries and probably the syntax. For example, in the employees' number input slot, one may specify that the letters comes before numbers and the maximum number of characters is 6. The specification ensures that a malicious user does not paste several input data in the entry (Nick, 2003).

Thus in conclusion, to apply input validation, one may consider applying white-lists/blacklists, canonicalization or check for content, among other methods.

Reference

Nick, S. (2003). Data Entry and Validation. New York, NY: Apress.