CITY OF MADISON INFORMATION TECHNOLOGY

Recommended Internal Controls for Microsoft Access

Overview

Effective: 08/01/2008

Amended: 07/06/2021

Objective: Ensure consistent internal control settings for agencies using Microsoft Access.

Purpose

Microsoft Access is a database management system (DBMS) that combines and contains the front-end application and back-end database within the same file (with an ACCDB file extension). Since the Access application file contains the application process business rules, the user interface (forms, reports) to the data, the database's metadata, the physical database itself, and the database engine, the controls to consider include not only the usual application control categories of input, processing and output controls, but also standard database controls. Since Access contains the application's Visual Basic for Applications (VBA) code and other database and application objects in the same file, the distinction between application controls and database controls becomes blurred.

Access is used globally to house business database applications. Access applications are often times completely unsecured or, at best, only partially secured. Therefore, many applications are easy to be altered or corrupted by an unauthorized user. Access has a variety of security tools and methods available to the designer that should implemented as soon as possible. Due to a lack of the many controls for a material financial database, Access is not recommended for this use (i.e., do not use this for payroll or tracking financial assets). For a well-controlled Access application, the following should be performed:

- The standard Ribbon should be replaced with a custom Ribbon.
- Controls must be present for data validation, inputs, and processing.
- The ACCDB file should be compiled to an ACCDE file.

This document outlines specific controls built-into Access and what can be done to securely manage databases. The following control categories will be discussed here:

1. Database Controls
2. Input Controls
3. Processing Controls
4. Output Controls
5. Auditing Controls

1. Database Controls

1.1. User Access Controls

In earlier versions of Access (pre-2007), you could create user accounts and passwords using a feature called user-level security. User-level security is not available in the newer .accdb file format.

1.1.1. Prevent unauthorized access to data tables and queries.

1.1.1.1. Encrypt a database by using a database password.

When you want to prevent unauthorized use of an Access database, consider encrypting the database by setting a password. If you know the password for an encrypted database, you can also decrypt the database and remove its password.

If you encrypt a database and then lose the password, you will be unable to use the database. You cannot remove a database password if you do not know the password.

For more information on how to encrypt/decrypt a database using a database password, please refer to the Microsoft support article.

1.1.1.2. There is a separate password to view and/or change the VBA code in general modules or class modules.

Access allows you to set a password to protect just the VBA code and not the rest of the database. Protecting the VBA code by using this procedure should not be considered a fool-proof security method. However, it's a good way to keep people from accidentally changing the code. A more robust way to protect the VBA code is to convert the database to an .accde file.

For more information on how to protect the VBA code, please refer to the Microsoft support blog.

1.1.1.3. The standard ribbon with its various administrator functions and permissions can be hidden and a customized ribbon inserted instead, thus denying access to many administrator or database owner powers.

The Ribbon – the strip across the top of the program window that contains groups of commands – is a component of the Microsoft Office user interface. As you build more advanced applications with Access, you may decide to customize the Office Ribbon to make the application easier to use or hide some of the default tabs so that users cannot use certain commands. You can also create new, custom tabs that contain only the commands that you want available.

The Ribbon can be customized using Extensible Markup Language (XML) or the built-in tools. The first route allows for customization possibilities, but it requires some basic knowledge of XML.

For more information on how to customize the Ribbon using XML, please refer to this Microsoft support article.

For more information on how to customize the Ribbon using the built-in Office tools, please refer to this Microsoft support article.

1.2. Development Tool Controls

1.2.1. Restrict or remove source code programming language and design view of database objects, so they cannot be viewed or changed by a user.

1.2.1.1. Start-up parameters are used to hide and/or disable design views of database objects, hide standard Ribbon, enable custom Ribbon tabs.

To reorganize, highlight, or hide database objects, you will need to create custom categories and groups in the Navigation Pane. For more information on how to customize the Navigation Pane, please refer to this Microsoft support article.

Please refer to 1.1.1.3. for information on how to customize the standard Ribbon.

1.2.1.2. A compiled version (ACCDE) of the ACCDB file can be created to remove user access to all database and application objects, including design views and VBA code.

A file with the .accde file extension is an Access execute only database file used to protect an .accdb file. It replaces the .mde format (which secures an .mdb file) used by older versions of Access (pre-2007). The VBA code in an .accde file is saved in a way that prevents anyone from viewing or editing it. When saving an Access database to the .accde format, you can choose to protect custom database code and encrypt the entire file behind a password. An .accde file also prevents anyone from writing changes to the reports, forms, and modules.

For information on how to create an .accde file and information on the format to consider, please refer to this Microsoft support article.

1.3. Data Concurrency Controls

1.3.1. Protect against deadlocks when two query or update processes access the same data item at the same time.

1.3.1.1. Multiple levels of data locking are available for concurrent users and can be set by the individual Access database administrator (DBA), and not IT.

The RecordsLock property determines how records are locked and what happens when two users try to edit the same record at the same time. There are three RecordLock properties that can be utilized: No Locks, All Records, and Edited Records.

For more information on the differences between RecordLock properties and how to enable them, please refer to this Microsoft support article.

1.4. Encryption Controls

1.4.1. Convert all clear text to encrypted text, which cannot be read and interpreted with any type of text editor.

1.4.1.1. The entire database must be encrypted/decrypted; encryption by a specific data field is not available.

Please refer to 1.1.1.1. for information on how to encrypt a database by using a database password.

1.5. Existence Controls

1.5.1. Protect the existence of the database by establishing backup and recovery procedures.

1.5.1.1. There are no available Access functions for backup or recovery; manual IT procedures or general network controls must be used for backup and recovery of entire Access database file.

*It is highly recommended to backup a database in case of system failure, file corruption, or simply when the **Undo** command isn't enough to fix a mistake. A backup copy may seem like a wasted use of storage space, but consider the time that might be saved by avoiding data and design loss. Creating backups on a regular basis is especially important when you have several users updating a database. Without a backup copy, you cannot restore corrupted or missing objects, or any changes to the database design.*

For more information on how to backup a database and when to plan them, please refer to this Microsoft support article.

1.6. Data Validation Controls

1.6.1. Ensure the accuracy, completeness, and consistency of data that are input and maintained in the database.

1.6.1.1. Table attributes can be assigned properties such as data type and size, data required (y/n), default values, input masks, and validation rules (e.g., value ranges).

Table attributes can be assigned a data type, input mask, validation rules, and more. Input masks ensure that users enter correctly format the data. Validation rules allow you to vet or validate data in Access desktop databases as you enter it. You can use the expression builder to help you format the rule correctly. Validation rules can be set in either table design or table datasheet view. There are three types of validation rules in Access: Field Validation Rule, Record Validation Rule, and Validation on a form.

For more information on input masks, please refer to this Microsoft support article.

For more information on validation rules, please refer to this Microsoft support article.

1.7. Audit Trail Controls

1.7.1. Provide a log (journal) of database activity of users and application events and data.

1.7.1.1. There are no available Access functions for audit trails or logs; application must provide custom programming for this.

Access does not have any built-in functions for creating and maintaining audit trails. This function can be programmed into the application by editing the VBA code.

2. Input Controls

2.1. Batch Controls

2.1.1. Protect integrity of data input by reconciling input number of records, hash totals, and monetary amount totals input to pre-input totals.

2.1.1.1. There are no available Access functions for batch controls; the application must provide custom programming for this.

Access does not have any built-in capability for input batch controls. This simple, yet effective, control must be programmed into the application by editing the VBA code and using SQL queries to compute, record, and display batch record counts, hash totals, and monetary totals.

2.2. Data Code Controls

Data code controls are very limited in Access and, in general, must be programmed into the application. One exception is to use input masks to control data entry formats. Please refer to 1.6.1.1. for more information on input masks.

2.2.1. Provide checks on the integrity of data codes, such as customer number or inventory number, by restricting input data to specifically allowed values; prevent transcription or transposition errors.

2.2.1.1. Specific required values from a drop-down list on the input form can be placed on the data item textbox.

2.2.1.2. Check digits are not specifically supported in Access; they must be programmed into the application.

2.3. Validation Controls

Setting table attribute properties for data validation control at the database level has already been discussed. Input data validation at the application level can be implemented by creating validation rules and validation error text attached to the data field textboxes on the data input form.

2.3.1. Ensure the accuracy, completeness, and consistency of input data items.

2.3.1.1. Input form data fields (textboxes) can be assigned physical properties, such as input masks or range tests.

Please refer to 1.6.1.1. for more information on input masks.

2.3.1.2. Input form data fields (textboxes) can be assigned a validation rule and error text.

Please refer to 1.6.1.1. for more information on validation rules.

2.3.1.3. The entire input form can be secured as read only, edit only, delete only, input only, or any combination.

2.3.1.4. Individual input data fields (textboxes) on forms can be secured by disabling and/or lockout.

3. Processing Controls

Access has no built-in capability for processing controls. Error messages and logs, run-to-run batch control totals, data code controls, validation controls, and the audit trail of processing steps must be custom-programmed into the application using VBA code operating on database objects (tables, queries, forms, reports, etc.). A well-controlled Access application would have all of these controls, and the absence of these controls would certainly indicate material weakness in internal control for the Access application and, therefore, perhaps other processes linked to the Access application.

3.1. Error Messages and Logs

3.1.1. Display and record appropriate information for any errors encountered during processing procedures.

3.1.1.1. There are no available Access functions for error logs; the application must provide programming for this.

3.2. Run-to-Run Batch Control Totals

3.2.1. Protect integrity of data processed by reconciling number of records, hash totals, and monetary amount totals before, during, and after processing steps, and compare to previously saved batch input totals.

3.2.1.1. There are no available Access functions for batch controls; the application must provide programming for this.

3.3. Validation and Data Code Controls

3.3.1. Ensure the accuracy, completeness, and consistency of data items processed.

3.3.1.1. There are no available Access functions at the processing step; the application must provide programming for this.

4. Output Controls

Access has no built-in capacity to control output distribution once it can be viewed or printed by a user.

4.1. Report Output Controls

4.1.1. Provide limitation over the production and distribution of reports.

4.1.1.1. There are no available Access functions for report distribution controls.

4.2. Display Output Controls

4.2.1. Provide limitation over the production and distribution to data in forms (i.e., screens and windows).

4.2.1.1. There are no available Access functions for display out controls

5. Auditing Controls

The following are suggested internal control questions to consider in regards to any material Access application. These questions do not by themselves make a professionally designed Access audit policy, but they act as a foundation for one to build upon. The more "yes" answers to the application questions means that the internal controls are stronger and the control risk is smaller.

Access internal control questions include:

5.1. Is the standard menu hidden and replaced by a custom menu that is absent all of the database application developer functions?

5.1.1. If the answer is "no," the application has serious control problems, since most of the other controls applied to the application can be compromised by the user's access to developer tools.

5.2. Is the installed application compiled to an ACCDE file?

5.2.1. If the answers to 5.1. and 5.2. are both "yes," internal control is definitely achievable in this Access application, although additional controls may be needed (see 5.3. through 5.12.).

5.2.2. If the answer to 5.1. is "yes," but the answer to 5.2. is "no," internal control is achievable, but many controls automatically available through a "yes" answer to 5.2.

5.2.3. If the answer to 5.1. is "no," but the answer to 5.2. is "yes," it is doubtful that control can be achieved due to the powerful development tools available to the ordinary user.

5.2.4. If the answers to 5.1. and 5.2. are both "no," then control is definitely not achievable.

5.3. Has a password been set up to restrict access to the VBA code found in general and class modules and procedures?

5.3.1. If the answer to 5.2. is "yes," this control is not needed if a compiled ACCDE file is created.

5.4. Has a single password needed to open the Access file been set up for all users?

5.5. Is the Access file encrypted?

5.6. Are data concurrency controls set up by the database administrator or owner? See 1.3. Data Concurrency Controls for more information.

5.7. Have data validation controls been set up at the table level for appropriate data fields?

5.7.1. Non-null data requirement?

5.7.2. Default values?

5.7.3. Data code drop-down lists for textboxes (if applicable)?

5.7.4. Input masks (if applicable)?

5.7.5. Data validation ranges, error text messages, and error logs?

5.8. Are run-to-run batch processing controls programmed into the application? See 3.2. Run-to-Run Batch Control Totals for more information.

5.9. Are audit trail controls programmed into the application? See 1.7. Audit Trail Controls for more information.

5.10. Are error log controls programmed into the application? See 3.1. Error Messages and Logs for more information.

5.11. Are existence controls (backup and recovery) in place (not really an application control)? See 1.5. Existence Controls for more information.

Conclusion

The above recommendations outline specific controls built into Access, and what can be done to securely manage databases.