Access Database Controls Security Framework and Audit Checklist

Are there (have there been) any Security Requirement Exceptions (SEC 501 1.5.0)?

Is it owned by, maintained by, provided by, coded by, or shared with any third party organizations?

Who is the
- System Owner
- Data Owner
- System Administrator
- Data Custodian

Determine
Year Placed in Service (Archer) – Look for audits or reviews since that date.

Version of Access Database

MS Support Calendar	Begin	End	Extended
Access 2007		10/10/17	
Access 2010	7/15/10	10/13/15	10/13/20
Access 2013	1/09/13	04/10/18	04/11/23
Access 2016	9/22/15	10/13/20	10/14/25

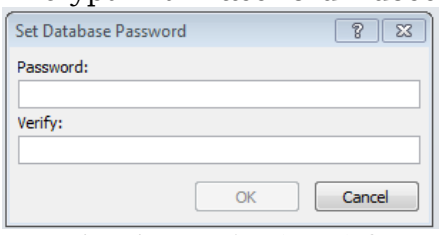
Compare Year Placed in Service to version of current DB. If deployed before version was available, there should be a clear trail of changes in the Change Management documentation. There should also be some form of source code control and testing or validation for the new release.

Examine file extension. If not an MDE or ACCDE, the application has not been compiled to prevent unauthorized changes.

To fully examine and test the application, both versions will have to be available. The MDE (compiled version) and the MDB (uncompiled version), or ACCDB/E equivalent.

In the MDB Version - Once the application is open:
Does the shift key bypass work (on open, use shift to bypass startup routine)?
Is the navigation pane visible? If not, does F11 work to show it?

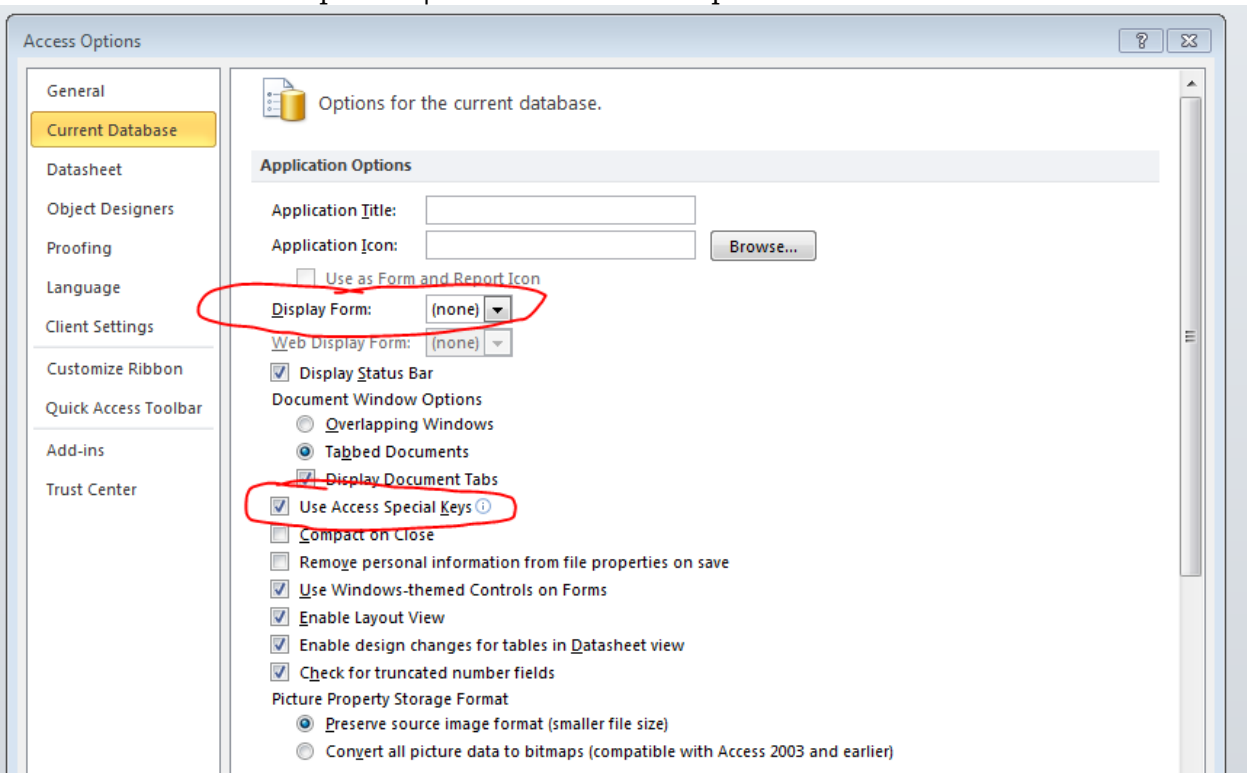
Security Model:
Encrypt With Password – does not meet AC requirements as login is shared



User-level security (ULS) features are not available in Access web apps, web databases, or databases that use one of the new file formats (.accdb, .accde, .accdc, .accdr). *ULS stopped as an added function with Access 2007.*

ULS now requires a custom module; there are third party plug-ins to leverage AD.

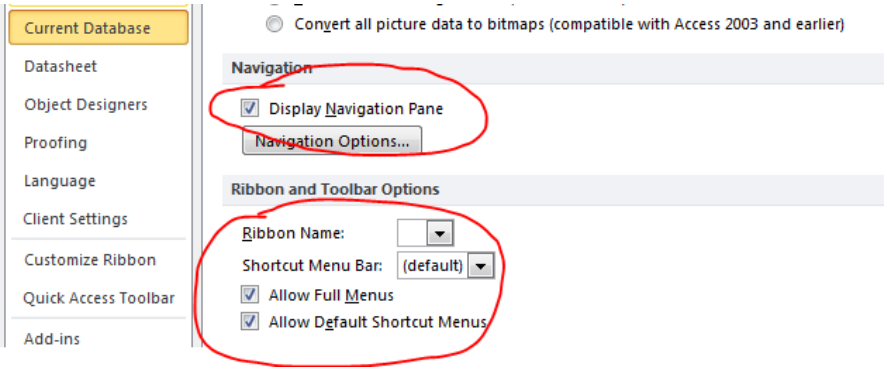
Examine the Access Options | Current Database parameters:



The Display Form selection should be used to start a menu option instead of giving complete access to the objects in the database.

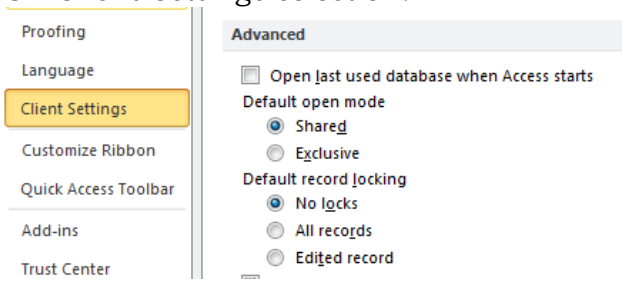
Use Access Special Keys should be turned off to stop short-cut keystrokes to enter menus and features.

Further down that same selection:



Navigation pane should be turned off. Ribbon should be custom and full menus off.

On Client Settings selection:



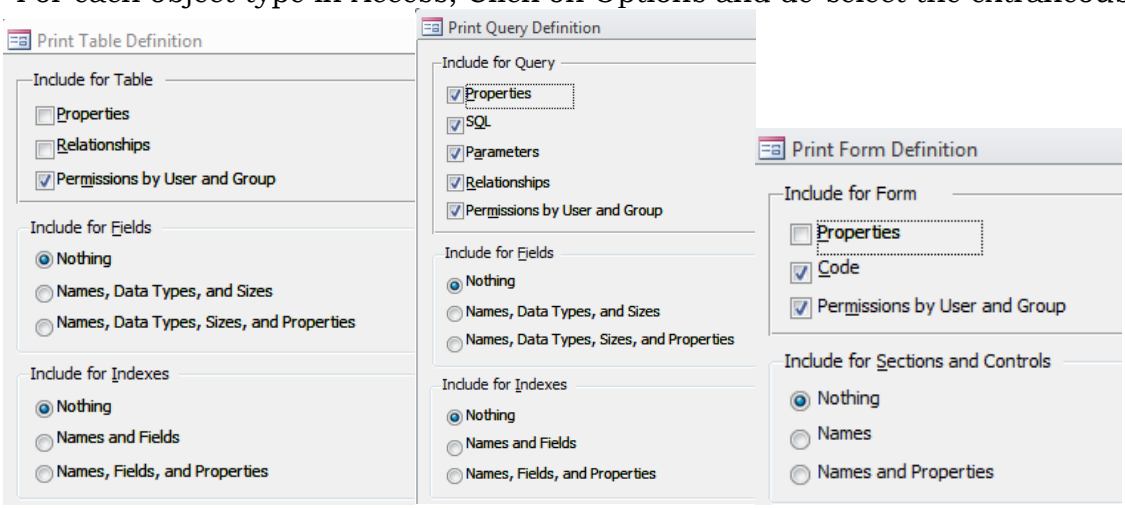
Default open mode should be Exclusive to prevent write/read errors.
Record Locking should be *at least* Edited Record, if not All Records

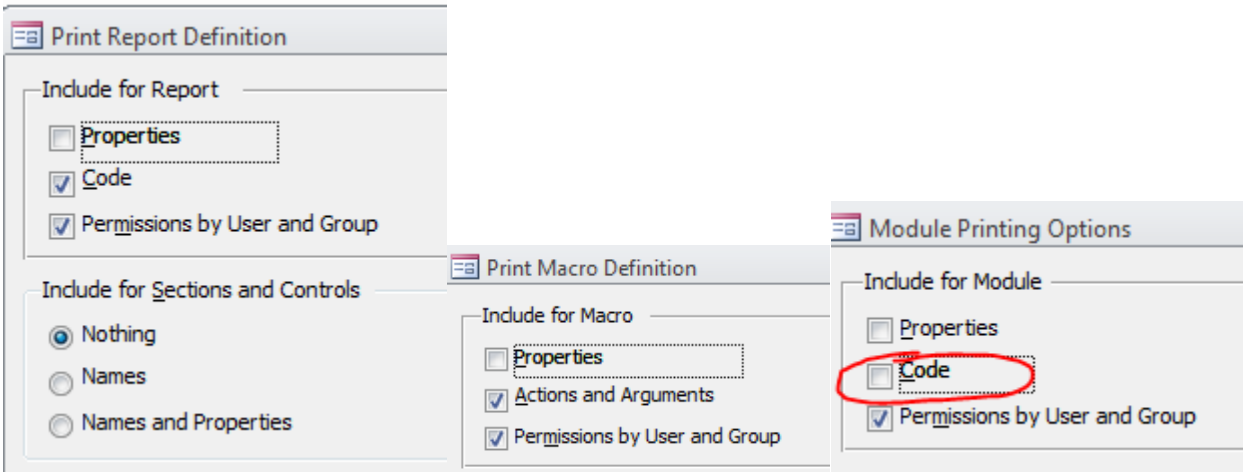
Examine Macros:
A Macro called Autoexec is executed each time the database file is opened. It can be set up to run anything – code, open/close objects, connection to external resources, refresh of attached data, etc.

Examine Navigation Options
Other than creating a custom interface for navigation, most programs will use the Switchboard Manager to enable a menu system for selecting user options. There should be a form call Switchboard in the object tree if this has been done.

Go to Database Tools tab on ribbon. Run Database Documenter* for all objects. Save report as PDF for examination and markup.

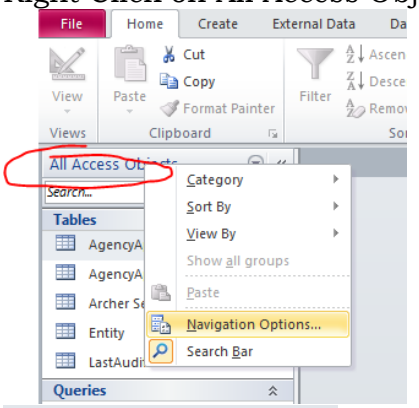
*For each object type in Access, Click on Options and de-select the extraneous data:

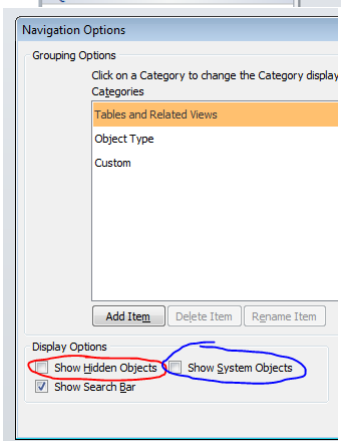




VB Code in Module Printing Options can render hundreds of pages of documentation, but it may be necessary at some point for comparison, debugging, or just reference. Interestingly – if printed (PDF), it can be used to rebuild the database code in case of corruption or loss.

Right Click on All Access Objects, then select Navigation Options*





Show Hidden Objects will enable objects that may contain sensitive or protected data, typically used to drive menus, drop-down lists and GUI forms that otherwise should not be in the user interface without invocation.

Show System Objects will reveal internal-operating repositories of data that often contain clear-text connection strings WITH passwords for attached resources (external access tables, excel files or RDMS objects).

*Can also get there from File | Options | Current Database |Navigation – click on Navigation Options button.

Audit trails and error logs/handling are not standard. Must be custom coded, tested, maintained and monitored.

Control Review

AC-1	Policy and Procedures
AC-2	Account Management
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-7	Unsuccessful Logon Attempts
AC-8	System Use Notification
AC-11	Session Lock
AC-12	Session Termination
AC-20	Use of External Information Systems
AU-1	Policies and Procedures
AU-2	Audit Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Audit Processing Failures
AU-6	Audit Review, Analysis, & Reporting
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-11	Audit Record Retention
AU-12	Audit Generation
AU-13	Monitoring For Info Disclosure
CM-1	Policies and Procedures
CM-2	Baseline Configuration
CM-2-COV	Additional Baseline Requirements
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-5	Access Restrictions for Change
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	IS Component Inventory
CM-9	Configuration Management Plan
CM-10	Software Usage Restrictions
CM-11	User-Installed Software
CP-1	Policies and Procedures
CP-9	Information System Backup
IA-1	Policies and Procedures
IA-2	Organizational Users
IA-4	Identifier Management
IA-5	Authenticator Management
IA-5-COV-1	Users and Devices
IA-6	Authenticator Feedback
PE-1	Policies and Procedures
PS-1	Policies and Procedures
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer
PS-7	Third-Party Personnel Security
PS-8	Personnel Sanctions
RA-1	Policies and Procedures
RA-3	Risk Assessment
SA-1	Policies and Procedures
SA-2	Allocation of Resources
SA-3	Life Cycle Support
SA-5	Information System Documentation
SA-8	Security Engineering Principles
SA-9	External Information System Services
SA-10	Developer Configuration Management
SA-11	Developer Security Testing
SA-15	Development Process, Standards, and Tools
SA-17	Developer Security Architecture and Design
SA-22	Unsupported System Components
SC-1	Policies and Procedures
SC-2	Application Partitioning
SC-3	Security Function Isolation
SC-4	Information in Shared Resources
SC-28	Protection of Information At Rest
SI-1	Policies and Procedures
SI-2	Flaw Remediation
SI-4	Information System Monitoring
SI-10	Information Input Validation