IT Security Questionnaire

1. What is used to store end user account information?
    a. MS SQL database?
        i. Is Password Rotation Supported?
        ii. Is Password Complexity Supported?
        iii. Are previously used passwords stored so they cannot be reused?
        iv. What method is applied to the passwords before storing? E.g. Encoding, Hashing, Encryption?
            1. If Encoding
                a. What is the need to have the password reversed?
                b. What is the timeline to have it changed to Hashing?
            2. If Hashing
                a. Is a salt used?
                b. What algorithm is used?
            3. If Encryption
                a. What encryption is used?
                b. What key strength?
                c. What is the need to have the password reversed?
                d. What is the timeline to have it changed to Hashing?
            4. Other method not listed? Explain:
    b. Active Directory?
        i. Can Active Directory Groups be used to limit access to who can run the application?
        ii. Can Active Directory Groups be used to limit access to certain applications functions
            1. Example, one user can make entries, but it takes another level of authorization from a manger to change entries.
        iii. If no on Active Directory, will the vendor modify the application to use Active Directory?
    c. Cloud?
        i. If cloud storage, where is the data geographically located?
        ii. Are any subcontractors located outside the US?
        iii. Are any employee's or subcontractor employees not US citizens?
    d. If not MS SQL or AD or Cloud, what is used for user account storage?
        i. If cloud storage, where is the data geographically located?
        ii. Are any subcontractors located outside the US?
        iii. Are any employee's or subcontractor employees not US citizens?

2. Does the application use a backend Database for storing data?
    a. What database system is used? MS SQL, Oracle, Cloud, etc.
        i. What version?

            1. If not the latest version, what is the timeline on getting to the latest version?
    b. Is any confidential (PCI, PII, HIPPA, other) data stored in the database?
        i. Is encryption used to protect confidential data?
        ii. Is any of the data regulated by any compliance or authority?
    c. Is any Database archiving done?
        i. If yes.
            1. What is the security applied to the Archive?
            2. Is any encrypted data decrypted for the archive?
            3. Is the archive stored in a location that is hardened as much as the live database?

3. How is an audit trail generated for activity?
    a. Where is the audit trail stored?
        i. MS SQL?
        ii. Offsite at the vendor (cloud)?
        iii. Local log files on the client?
        iv. Archived PDF Documents?
    b. How long is the audit trail stored?
    c. Is any confidential information stored in the audit trail?
    d. Is any encryption used on the audit trail storage?
    e. Does the audit trail contain
        i. Date/time of alteration.
        ii. User that performed alteration.
        iii. Parameter altered
        iv. Value prior to alteration
        v. Value after alteration
    f. How do we view the audit trail?

4. Does the application need Internet Connectivity?
    a. If yes, is the communication over SSL?
    b. If yes, what data is being pulled/sent to the Internet?

5. After installation, does any part of subsystem of the application require Windows Local Administrator Rights to run?
    a. If yes, is the vendor willing to correct this flaw?

6. How does the client application talk to the server backend? E.g. Direct connection to a database, through web/app service, etc.
    a. If direct connection to DB, Does the client use Ad Hoc or Stored Procedures?
        i. If Ad Hoc at all, can application run on just stored procedures?

    b. If direct connection to DB, what authentication method? E.g. DB/Local User or Windows Integrated.
        i. If DB/Local User, how are credentials stored on client?
            1. Are they encrypted?
        ii. If DB/Local User, what connection client is used? ODBC, SQL Native, etc.

7. Is any encryption used in communications between machines in the system? E.g. Between client and server, between application server and database server.
    a. If no, can it be implemented?
    b. If yes, which communication channels and what level of encryption and algorithm are used? E.g. Client to Server- AES256, Client to Web Server - SSLv3 2048
8. Does any part of the backend system require a console application to be left running in the background on the "server" at all times?
    a. What is the timeline to correct this defect?

9. Do the client workstations run in kiosk mode (1 generic user logged into machine, many users log into application) or can the application run under the logged in user with any valid user logging into the machine?
    a. If yes to kiosk mode, can the application be changed to allow running under any logged in user?

10. Is alerting supported on "odd" behavior? E.g. anything that falls outside of a configurable threshold on the system or unusual activity that goes outside of a normal process.
    a. What kind of alerting or mitigating measures can be used in the event of such behavior or threshold breach?
11. Is any form of file share required (on client or server) for the application to operate?
    a. If yes, what levels of permissions are required and who will need them?

12. If using a Database, are the DB vendors (Microsoft/Oracle/etc) Best Practices for securing the database server followed? In other words, if a server was set up with Best Practice guidelines, does any of it need to be "loosened" in order for the application to work?
13. Are the Client/Server Operating System (OS) vendors Best Practices for securing the OS in its particular role followed?

14. Is regular patching of the Client and Server OS with the latest vendor patches and service packs supported?

15. Is regular patching of the Database Server with the latest vendor's patches and service packs supported?

16. Does the application meet all required regulatory compliances? E.g. TICS, PCI, HIPPA, ITAR, etc.?