**Aspekt Demo Session – April 12 – 13, 2022**

**AAA questions by team**

|  |  |  |
| --- | --- | --- |
| **Row No** | **Question** | **Answer** |
| **Information Security Questions** | | |
| **1** | Can we implement MFA? | Can be customised.  MFA is currently unsupported in the ASPEKT Product Suit, but it can be developed upon request.  The ASPEKT Mobile App supports MFA however. |
| **2** | Do you encrypt the passwords in the system? | ASPEKT Product Suit doesn’t store the user’s passwords at all.  Users are created on the Active directory or in the SQL Server, depending on the chosen authentication model by AAA. |
| **3** | Can we implement custom password policy? | Fully Supported.  Both the Active Directory and the SQL Server allow custom password policies. AAA can determine the desired password policy and ASPEKT’s core solution will abide by it. |
| **4** | Can we create role based users? | Fully Supported.  Roles can be created and modified by AAA (within predetermined Role Types). Furthermore, privileges to Roles can also be managed and multiple roles can be assigned to a single user, all by AAA . |
| **5** | If yes Can admin change their roles anytime? | Fully Supported.  AAA Admin user can add new roles to a certain user and grant/deny existing roles. |
| **6** | Do the system give alert before a certain number of days for password change before it gets expired Login (user cannot log in parallel from other computers)? | AAA can determine the maximum days of password validity in the Active directory or the SQL Server and AAA core solution will notify the user prior password expiry by reading the information.  As this is a centralised process in the ASPEKT Product Suit, the user can not log in from another computer successfully. |
| **7** | Can user use 2 or more sessions in the same time? | The system allows the user to use multiple sessions.  AAA can limit the use to only one session by setting the appropriate parameter within the solution. |
| **8** | Can you provide standard login and logout controls like lock account after certain number of wrong attempts, logout after a specified time and one time password for temporary users etc? | AAA determines the maximum number of wrong attempts for account lock in the Active directory or the SQL Server.  Within the ASPEKT Product Suit, an Admin user can access the information/reason behind the locking and can reset the password directly. |
| **9** | Are data encrypted before sending it over the Internet or an open network? | ASPEKT requires to have an SSL certificate on the Application server for encrypted communication (https) between the Front application and the Server Application.  ASPEKT does not encourage using the CBS system over an open network (Internet), but rather by using a VPN or a local network for Front Application and Server Application.  Of course, this is mainly the decision of AAA. |
| **10** | Are audit log files protected from unauthorized alteration including by admin? | Audit logs are kept on a minimum of two separate locations. Files (for application logs) and database (for application logs and database logs - changes into tables).  All logs can be additionally transferred to other dedicated systems like TSIEM systems  (setup should be performed beforehand by AAA team). ASPEKT has no access to either of the locations and can’t interfere if someone modifies certain data in all locations.  Authorization or unauthorization on AAA systems is managed by AAA and ASPEKT is not involved in restricting the permissions on file system level or Active Directory/SQL level. |
| **11** | Is the application time stamp for audit log entries synchronize with other applications and systems using NTP/SNTP? | ASPEKT Product Suit is using the server’s operating system time and all logs are written with the exact time. The operating system time should be synchronised via NTP /SNTP services. |
| **12** | Can we export audit logs for further usage (SIEM, analyse, store)? | Export is available in the following formats: Excel and Tx. Additionally the SQL tables where the data is stored can be used for further analysis. |
| **13** | Can admin set the inclusion or exclusion of audited events based on organizational policy and operating requirements or limits? | At database level, the system administrator can allow/deny triggers.  For the audit log, the system administrator can add or remove services that need to be monitored. Changes for the audit log should be applied in a configuration file - appsettings.json. |
| **14** | Is it possible to mask some information fields in log entries before they are sent to SIEM? | ASPEKT enables the possibility to set a list of information fields (E.g. email, personal number etc.) that should be modified, masked or deleted prior being sent to log. Changes for the audit log should be applied in a configuration file - appsettings.json. |
| **Business Continuity Questions:** | | |
| 1 | Can each module (GL, transactions, fixed assets, balance sheet, credit portfolio etc.)  work separate of each other? If one model down, will it affect the other modules? | The solution is designed to function on a modular level and momentary interruptions in one module do not affect the overall solution. Additionally, this allows newly purchased modules to be easily added to the solution. |
| **2** | Is there an ability to run a backup concurrently with the operation of the application? | ASPEKT Product Suit’s binary and configuration files residing on the application servers can be safely backed during normal application operation and without any impact on the working processes with the solution. |
| **3** | Does the functionalities continue normal operation even when security audit capability is non-functional? | Audit Logs are asynchronous and have no impact on normal operation of processes within the solution |
| **4** | Are updates controlled by an agreement? | Any update is performed with previously obtained permission and by providing a Release note containing all changes that are taking place. |
| **5** | Did you test to be fully functional residing on its associated operating system/middleware platform configured with a recognized security configurations? | The following four System Environments are required and used to achieve optimum functionality:  1. Testing Environment - test application (without migrated data) used for testing new features and versions  2. Training Environment - used for training purposes (with customised data)  3. Pre-production Environment - full functional application with production or anonymous data  4. Production Environment |
| **6** | Will you notify us before updates? | Any update is performed with previously obtained permission and by providing a Release note containing all changes that are taking place. |
| **7** | Are you able to provide our users and system administrators with documentation that explains error or messages information on what actions are required? | Aspekt Product Suit has implemented Global Error Handling where all Error messages are kept and stored in the database. On previously agreed time intervals the ASPEKT team monitors and investigates frequently appearing Errors to provide solution or advice on actions to be taken. |