|  |  |  |
| --- | --- | --- |
| ectu logo no script | <<Project Name>>  Risk Assessment |  |

### Document History

|  |  |  |
| --- | --- | --- |
| Date | Version Author(s) and project roles | Reason |
| <<Date Created> | <<Your name>> (CDMA Developer) | * Initial creation |

| Identified Risk | Why is this a risk? | Category | %age Likelihood | Mitigators in Place |
| --- | --- | --- | --- | --- |
| Database server file corruption | The trial’s data can no longer be accessed from the database server. The data is effectively lost. | Database Server | <1% | 1. Database server Backup regime in place. This backs up the data and the database file can be recovered. |
| Server Unavailable. This could be the Web Server or the Database Server | System users cannot access the system to enter data or perform randomisation if the database server is unavailable. | Server Availability | 5% | 1. Each trial to have a procedure in place about what steps to take in the event a randomisation needs to take place when the database server is unavailable. |
| Unauthorised Physical Access to Servers | Unauthorised personnel could physically damage or remove the server or any of its components.  Introduce additional hardware components | Server Security | <1% | 1. Servers are held within a secured environment with physical access limited to approved personnel. |
| Unauthorised Logical Access to Servers | Unauthorised logical access exposes the trial data in unplanned ways jeopardising the integrity of the data. | Server Security | 5% | * Logical access to servers is limited to named IT personnel attached to a specific role. * Servers are software patched in accordance with vendors’ guidelines. |
| Network Unavailability | System users cannot access the system to enter data or perform randomisation if the database server is unavailable users will not be | Infrastructure | <1% | 1. Each trial to have a procedure in place about what steps to take in the event a randomisation needs to take place when the database server is unavailable. |
| Website SQL Injection attacks | Attacks expose the database server and thus critically jeopardise the trial data | Internet-based Maliciousness | 100% | Authenticate CDMA website access.  Build all data access mechanisms using prepared statements/stored procedures rather than SQL strings |
| Cross Site Javascript Attacks | These are internet-based site ‘hijack’ attempts. A successful attack tricks the CDMA into running code scripts that were written by unauthorised personnel | Internet-based Maliciousness | 100% | * Validate all input including posted data and query strings. * Use ASP.NET framework to develop web sites. This has built-in protection for this kind of attack. |
| Internet traffic sniffing | The website CDMA communicates with users across the internet. If this communication is intercepted and decoded the trial’s data is critically jeopardised. | Internet-based Maliciousness | 100% | The SSL protocol is imposed for all communications between the CDMA and the user. This protocol is an industry-standard protocol for encrypting data across the internet. |
| Unauthenticated access to data | Exposes the trial’s dataset to unexpected personnel.  So unauthorised personnel can view and change the trial’s data set. | General System Security | <1% | Username/password authentication |
| Unauthorised access to data | Clinical trials often collect data for participants at different sites. Site researchers should only have access to their own site’s data set.  For site researchers and other personnel dealing directly with participants access to unauthorised data can jeopardise the trial’s ‘blindedness’ and introduce ‘Information Bias’ that would jeopardise the trial’s outcome. | General System Security | <1% | Role Based security  Site based security |
| System collects the wrong dataset | Collecting the wrong dataset affects the integrity of the trial. There is a risk that the dataset cannot answer the scientific questions posed by the trial designers | Dataset definition | 50% | CRF meetings are arranged with stakeholders to finalise the CRF prior to the trial CDMA being developed.  Any changes to the dataset are reviewed and approved prior to being introduced to the ‘live’ system. |
| System doesn’t retain the dataset correctly | The trial’s ‘back-end’ database doesn’t contain the data set expected, so the trial analysis cannot proceed and the trial outcome could be affected. | CDMA Design and Development | <1% | Each section of the CDMA, prior to it going live goes through a validation process.  Key data sets go through a quality control process after data entry.  Interim analyses are carried out by statisticians prior to the trial reaching the final analysis stage. This provides additional quality control. |
| Front-end features don’t operate as expected.  ‘Front-End’ is the main bulk of the CDMA. It’s that part of the system visible to the users of the CDMA. | The system not behaving as expected jeopardises the data set being collected.  This risks the trial being unable to answer the scientific question posed by the trial. | CDMA Design and Development | 50% | Each section of the CDMA, prior to it going live goes through a validation process.  Any changes to the CDMA are reviewed and approved prior to being introduced into the ‘live’ system. |
| Treatment allocation process doesn’t operate as expected  The design of all clinical trials is based upon the allocation of participants to the appropriate groups as dictated by the trial protocol. | Failure of the treatment allocation mechanism may very well stop the trial being analysed according to its set out plan. This will jeopardise the ability of the trial to answer the scientific questions of interest. | CDMA Design and Development | 5% | The trial’s treatment allocation process undergoes validation through an automated testing mechanism designed and implemented specifically for the trial.  This testing mechanism ensures the state of the database tables after each treatment allocation is as expected. |
| Requirements changing during initial system development | It increases the development timeline. This can jeopardise the recruitment phase. The main area of churn is in the development of the CRFs | CDMA Design and Development | 100% | CRF meetings are arranged with stakeholders to finalise the CRF prior to the trial CDMA being developed |
| Requirements changing after the system goes live. | Increases the lifetime cost of the project CDMA.  Increases the risk of errors being introduced to the system.  May involve changing the trial’s dataset. This could lead to inadvertent data loss or corruption.  Changing the system can introduce further training requirements for users | CDMA Design and Development | >90% | Controlled process for requesting and implementing system changes.  Includes:  Formal change request system.  Acceptance of change request.  Changes are implemented within a separate staging environment.  Changes are validated and approved prior to being introduced to the live system. |