|  |  |  |  |
| --- | --- | --- | --- |
|  | **Knee planning** | **Knee Intra-op** | **Knee balancer** |
| Platform | Runs on a separate laptop | It runs on Nav3i, Qcart, OrthoQ cart | Runs on ipad/iphone |
| OS | Windows | Windows/Linux | MAC/iOS |
| Execution stage | Pre-operative data | Intra-operation data | Pre-operative data |
| Input device | ? | USB, (CD?) | MAKO system |
| Input format | ? | TDM file/DICOM image | MAKO system -> Image ->Values |
| Output | Anonymized output | No output | Algo generated solns |
| Authentication |  | Windows authentication | Downloads from SYK store |
| Users | MKS user | Surgeon | Surgeon |
|  |  |  |  |
|  |  |  |  |
| AC-Access control  (complete family) | The application (CT based Knee Planning software) has no dedicated access control functionality (enabling account management, separation of duties, least privilage, session locks, etc.)  The application is running under a Windows OS system and is managemend by according Windows access controls and by HDOs (Health Delivery Organization) IT department | -No dedicated access control functionality |  |
| AT- Security awareness & training  (complete family) |  |  |  |
| AU- Audit & accountability  AU-1 Audit & accountability policy and procedures  AU-2 Audit events  AU-4 Audit storage capacity  AU-6 Audit review, analysis and reporting  AU-7 Audit reduction and reporting generation  AU-10 Non-repudiation  AU-11 Audit record retention  AU-12 Audit generation  AU-13 Monitoring for information disclosure  AU-14 Session audit  AU-15 Alternat audit capacity  AU-16 Cross-organizational auditing |  |  |  |
| CA-7 continuous monitoring |  |  |  |
| CM- Configuration management  (complete family) |  |  |  |
| CP- Contingency planning  (complete family) |  |  |  |
| IA- Identification & Authentication |  |  |  |
| IR- Incident Response  IR-9 Information spillage response  IR-10 Integrated information security analysis team |  |  |  |
| MA- Maintenance  (complete family) |  |  |  |
| MP- Media Protection  (complete family) |  |  |  |
| PE- Physical & environmental protection  (complete family) |  |  |  |
| PL- Planning  PL-7 Security concept of operations  PL-8 information security architecture |  |  |  |
| PM- Program plan  PM-15 Contacts with security groups and associations |  |  |  |
| SA- System & service acquisition  SA-1 System & service acquisition policy and procedures  SA-4 Acquisition process  SA-5 Information system documentation  SA-9 External information system services  SA-12 Supply chain protection  SA-13 Trustworthiness  SA-14 Criticality analysis  SA-15 Development process, standards & tools  SA-16 Developer provided training  SA-17 Developer security architecture & design  SA-18 Tamper resistance & detection  SA-21 Developer screening |  |  |  |
| SC- System & communication protection  SC-1 System & communication protection policy & procedures  SC-7 Boundary protection  SC-8 Transmission confidentiality & integrity  SC-12 Cryptographic key establishment and management  SC-13 Cryptographic protection  SC-17 Public key infrastructure certificates  SC-25 Thin nodes  SC-26 Honeypots  SC-29 Heterogeneity  SC-30 Concealment & misdirection  SC-31 Covert channel analysis  SC-34 Non-modifiable executable programs  SC-35 Honey clients  SC-37 Out-of-band channels  SC-40 Wireless link protection  SC-41 Port and I/O device access  SC-42 Sensor capability and data  SC-43 Usage restrictions  SC-44 Detonation chambers |  |  |  |
| SI- System & information integrity  (complete family) |  |  |  |
|  |  |  |  |