|  |  |  |  |
| --- | --- | --- | --- |
| S.no | Control | Assessment changed (by reviewer) to | Include changed (by reviewer) to |
| 1 | AC-8 System use notification | NO | - |
| 2 | AC-11 Session lock | YES | - |
| 3 | AC-17 Remote access | YES (YES in planning) | YES |
| 4 | AC-18 Wireless access | YES (YES in planning) | YES |
| 5 | AC-19 Access control for mobile devices | NO | - |
| 6 | AU-10 Non-repudiation | YES | - |
| 7 | CA-7 Continuous monitoring | YES | YES (YES in planning) |
| 8 | IR-1 Incident response policy and procedures | - | YES (YES in planning) |
| 9 | IR-2 Incident response training  For example, regular users may only need to know who to call or how to recognize an incident on the  information system; **system administrators** may require additional training on how to handle/remediate incidents; and **incident responders** may receive more specific  training on forensics, reporting, system recovery, and restoration. | - | YES (YES in planning) |
| 10 | IR-3 Incident response testing  for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive  exercises. | YES | YES (YES in planning) |
| 11 | IR-4 Incident handling  for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events | YES (YES in planning) | YES (YES in planning) |
| 12 | IR-5 Incident monitoring  for example, maintaining records about each incident, the status of the incident, and other pertinent  information necessary for forensics, evaluating incident details, trends, and handling. | YES (YES in planning) | YES (YES in planning) |
| 13 | IR-6 Incident reporting  for example, the receipt of suspicious email communications that can  potentially contain malicious code. | YES (YES in planning) | YES (YES in planning) |
| 14 | IR-7 Incident response assistance  for example, help desks, assistance groups, and access to forensics services, when required. | - | YES (YES in planning) |
| 15 | IR-8 Incident response plan  for example, external service providers  and organizations involved in the supply chain for organizational information systems. | - | YES (YES in planning) |
| 16 | PE-1 Physical and environmental protection policy and procedures | YES | YES |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.no | Control/Control family | Justification | Source | Comments |
| 1 | AC family | Modified | - |  |
| 2 | AT family | Changed | Knee Planning | Just used the justification from the planning appl |
| 3 | AU (13,14,15,16) | Modified | - | Shouldn't we argue like:  This is to be addressed by the HDO policy since the application is running on a Platform which is governed by the HDO's IT.  But the application is supporting the HDO's need for auditing by creating and providing a log file which is recording actvities within the application |
| 4 | CA-7 Continuous monitoring | - | - | Also, shouldn't we argue like:  Since the application is running on a Platform which is governed by the HDO's IT this requirement should be considered in the HDO security policy |
| 5 | CP family | Modified | Knee planning |  |
| 6 | IR (1,2,3,4,5,6,7,8) | - | - | I would uset the same approach as we did for the planning application |
| 7 | IR-9 Information spillage response | - | - | Didn't understand |
| 8 | IR-10 Integrated information security analysis team | - | - | Contradics the Corporate procedure |
| 9 | MA family | - | - | General comment concerning Nav 3i:  1. The submission combines Intra OP and Nav 3i  2. The customer does not care about who in Stryker did the Platform and who the application  That's why you inherit the responsibility for features which are considered in Nav 3i and provide security for the overall packegae |
| 10 | PE family | Changed | Knee planning | Used the same defintion as we established for plannign since the HDO IT has to care about phys. Securitz (e.g. certain cabinets for the Med. Devices which are protected |
| 11 | PM-15 Contacts with security groups and associations | - | - | Are you sure? |
| 12 | PM-16 Threat awareness program | - | - | Again - I would align here with the planning app. |
| 13 | SC-30 Concealment and misdirection | - | - | why? |
| 14 | SC-43 Usage restrictions | Modified | - | Didn't understand |
| 15 | SI (1,2,3,4,5,6,7,8) | - | - | Contradiction to some controls before and to the planning app |

|  |  |  |  |
| --- | --- | --- | --- |
| S.no | Control |  | Comments |
| 1 | CP-9 Information system backup |  | Does the platform support backups? |
| 2 | CP-10 Information system recovery and reconstitution |  | Does the platform support recovery? |
| 3 | SA-13 Trustworthiness  the degree to which the system can be expected to preserve the confidentiality, integrity, and  availability of the information it processes, stores, or transmits. | YES (Include tab) | What did you have in mind here? |
| 4 | SA-17 Developer security architecture and design  This distinction is important if/when organizations outsource the development of information systems, information  system components, or information system services to external entities, and there is a requirement to demonstrate consistency with the organization’s enterprise architecture and information  security architecture. | YES (Include tab) | Why yes? |
| 5 | SA-18 Tamper resistance and detection  Anti-tamper technologies and techniques provide a level of protection for critical information  systems, system components, and information technology products against a number of related  threats including modification, reverse engineering, and substitution. | YES (Include tab) | Why yes? |
| 6 | SC-8 Transmission confidentiality and integrity  applies to both internal and external networks and all types of information system  components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). | YES (Include tab) | Why? |
| 7 | SC-12 Cryptographic key establishment and management  includes certificates with visibility external to organizational  information systems and certificates related to the internal operations of systems. | NO (Include tab) | Why no yes? |
| 8 | SC-13 Cryptographic protection  for example,  the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the  necessary clearances for such information but lack the necessary formal access approvals | NO (Include tab) | Why no yes? |
| 9 | SC-28 Protection of information at rest  System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. | NO (Include tab) | Contradicts planning app. There is an according SRS requirement |
| 10 | SC-41 Port and I/O device access  Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. | YES (Include tab) | Why? |
| 11 | SI-10 Information input validation  Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match  specified definitions for format and content. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.  SI-11 Error handling  for example, erroneous logon attempts with passwords entered by mistake as the username,  mission/business information that can be derived from (if not stated explicitly by) information  recorded, and personal information such as account numbers, social security numbers, and credit card numbers.  SI-12 Information handling and retention  Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems.  SI-15 Information output filtering  focuses on detecting extraneous content, preventing such  extraneous content from being displayed, and alerting monitoring tools that anomalous behavior  has been discovered.  SI-17 Fail-safe procedures  for example, alerting operator personnel and providing specific instructions on subsequent steps  to take (e.g., do nothing, reestablish system settings, shut down processes, restart the system, or contact designated organizational personnel). | YES (Include tab) | Which are the thoughts behind the following Yeses? |
|  |  |  |  |

**Corporate Policies:**

|  |  |  |
| --- | --- | --- |
| S.no | Control/Control family | Traceability |
| 1 | IR family | D0000003113, Product Security Post Market Management |
| 2 | PM-16 Threat awareness program | D0000003113, Product Security Post Market Management |
| 3 | PL family | post market surveillance |
| 4 | PS-1 Personnel security policy and procedures | Corporate QMS product security policy and procedures |
| 5 | SA-3 System development life cycle | D0000061606 Security and privacy in design controls |
| 6 | SA-5 Information system documentation | User Manual (D005010067), IFU(D005010049) and Security Operations Manual(D005010066) |
| 7 | SA-8 Security engineering principles | D0000061606 Security and privacy in design controls" and "D0000061607 Privacy by design |
| 8 | SA-10 Developer configuration management | (D0000061620: Section 5)Configuration management in Software Development plan |
| 9 | SA-11 Developer security testing and evaluation | D0000061606 Security and privacy in design controls |
| 10 | CA-7 Continuous monitoring | D0000003113 requires in 7.2.1.3 Surveillance for potential vulnerabilities as determined by Deivisions before production release |
|  |  |  |
|  |  |  |