| **Control[[1]](#endnote-1)** | **Design Effectiveness[[2]](#endnote-2)** | **Type & Freq.[[3]](#endnote-3)** | **Key Control[[4]](#endnote-4)** | **Test[[5]](#endnote-5)** | **Op**  **erational Effectiveness[[6]](#endnote-6)**  (Test Conclusion) | **Report Disposition[[7]](#endnote-7)** |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk A – Access Management**  Lack of management oversight of implemented processes and controls to address authorized access controls could lead to the vulnerability of data. | | | | | | |
| **A.1 – Access Control**    **Effective control over access to computer functions and related data is dependent on the use of the application’s security feature and/or access-control.**  ***Control Owner: Ken Park, Sr. Director, RxClaim Development, PBM IT Systems.*** | **Effective** | A  P  As Needed | Yes | Performing Testing to ascertain:   1. Access to claims data is limited to appropriate personnel/stakeholders/individuals 2. Ensure user access is authorized and appropriately established (New User/Set-up/Provisioning). Policy governing access for new personnel. 3. Review security packages access-controls definitions, logon IDs and associated privileges, authentication methods, access and resource rules, for appropriateness. | [*Test Conclusion – See Methodology*] | [*Reportable Disposition of any gaps or exceptions*] |
| **Risk B – Override Capabilities**  Without a controlled process for overrides, application changes, inappropriate or unauthorized changes could negatively impact the availability, security, and integrity of the environment | | | | | | |
| **B.1 – Override**    **Override of computer edits involves intervention by the application owner by allowing the user the capability to bypass what under normal conditions would be an error that would prevent processing of the transaction to proceed.**  ***Control Owner: Ken Park, Sr. Director, RxClaim Development, PBM IT Systems.*** | **Effective** | M  D  As  Needed | Yes | Performing Testing to ascertain:   1. Review the use of override to determine that it is restricted to an authorized user and that an audit trail if its use is properly recorded. 2. Review the access/resource rules that control who can use the override capability. | [*Test Conclusion – See Methodology*] | [*Reportable Disposition of any gaps or exceptions*] |

|  |  |
| --- | --- |
| **Scope Objective Reference** | |
| SO-1 | Access Management |
| SO-2 | Override Capabilities |

1. Be sure the control mitigates the assigned risk and that all controls have all five components of a control (1. person / process; 2. performing a function; 3. frequency; 4. prevents or detects; 5. evidenced). If one of the five is missing, verify with SME that the component is not otherwise addressed. If so, then note the Control Gap (note what component the control is lacking). [↑](#endnote-ref-1)
2. If all five components of a control are addressed and the control mitigates the risk, then it is an "Effective" control. If it does not mitigate the risk, it might be a process. If it does not include all five, this is a control gap and "Control Gap" should be noted. [↑](#endnote-ref-2)
3. A = Automatic Control (performed by a system); M = Manual Control (performed by a person); D = Detective (the control identifies instances of the realized risk after the fact)

   P = Preventative (the control mitigates the risk from occurring); How often is this control performed: Daily (once a day or more); Weekly; Monthly; Quarterly; Annually. [↑](#endnote-ref-3)
4. Key Control: substantially mitigates the risk on its own. Non-Key Control: supports a key control, but cannot wholly mitigate the risk on its own. [↑](#endnote-ref-4)
5. Describe the test steps to determine whether an effectively designed control is operating effectively. Be sure to include the following: 1. Define sample size (usually 25% of population) and testing sample (if possible). 2. Include the specific name of any reports referenced. 3. Verify the test addresses the risk (does it address completeness, accuracy, and / or timeliness). If the control is not effective, note "No testing to be performed due to ineffective control." [↑](#endnote-ref-5)
6. Describe the outcome of the test, clearly stating that the control either Passed or Failed the test. [↑](#endnote-ref-6)
7. Describe the impact the Design Effectiveness and Operational Effectiveness results have on the audit report. List how the findings are included within any reportable issues. If findings were not reportable, explain relationship for the non-reportable disposition. [↑](#endnote-ref-7)