



**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

**PROJECT DEVELOPMENT AUDIT PLAN**

Our objectives are to assist in the development of effective and efficient controls during the implementation of the new system. In that regard, we will follow these general guidelines –

- Contact business owner(s) responsible for the target project and inform them of your involvement in the project.
- Arrange to attend project-planning meetings.
- Request and review copies of project plans, action plans, issues lists, resource plans, status reports, flow charts, procedure write-ups etc., to determine that sufficient documentation exists to control and monitor the project.
- If the above requested documentation is not available or insufficient, immediately bring those to the attention of the responsible manager and recommend the documentation be created as appropriate. Also note the recommendation on the Project Scorecard.
- Continue receiving and reviewing updated versions of the above documents throughout project.
- Assess actions being taken and progress being made to address project issues. If progress is not being made (target dates not met, functionality not achieved) immediately bring those problems to the attention of the responsible manager, and recommend additional actions as appropriate, on the Project Scorecard.
- Look for risks and gaps that may not have been identified or not considered (missed) by the area. If found, immediately bring your concerns to the attention of the responsible manager and the project leader. Share with the manager any recommended actions you think should be taken to address the risks/gaps, and also note them on the Project Scorecard.
- As appropriate, test samples of source documents processed by the system or manually to ensure that systems and processes are working as intended. If errors are detected, immediately bring the errors to the attention of the responsible manager. Share your recommendations with the manager and also note them on the Project Scorecard.

<u>Procedure</u>	<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
<b>Section I - Project Management</b>			
<b>I. PRELIMINARY PROCEDURES – General Guidelines</b>			
A. Contact business owner(s) responsible for the target project and inform them of your involvement in the project.			
B. Arrange to attend project planning meetings			
C. Request and review copies of project plans, action plans, issues lists, resource plans, status reports, flow charts, procedure write-ups etc., to determine that sufficient documentation exists to control and monitor the project.			
1. If the above requested documentation is not available or insufficient, immediately bring those to the attention of the responsible manager and recommend the documentation be created as appropriate			

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
D.	Assess actions being taken and progress being made to address project issues. If progress is not being made (target dates not met, functionality not achieved) immediately bring those problems to the attention of the responsible manager, and recommend additional actions as appropriate			
E.	Look for risks and gaps that may not have been identified or not considered (missed) by the area. If found, immediately bring your concerns to the attention of the responsible manager and the project leader. Share with the manager any recommended actions you think should be taken to address the risks/gaps			
F.	Are HIPAA impacts considered and coordinated with the HIPAA Governance Committee?			
<b>II. PROJECT MANAGEMENT – To determine if there is an adequate level of project management support</b>				
A.	Determine the makeup, authority and support of the project team.			
1.	Are the respective Project Leaders well versed in project management methodology?			
2.	Is the appropriate level of management involved in the project?			
3.	Does the project team include members from all user areas?			
4.	Does the project team have the appropriate level of expertise, including IT and business operations?			
B.	Determine if a formal project request has been initiated.			
1.	Was a formal project request generated?			
2.	Does the request include documentation of the expected benefits to be achieved?			
3.	Is a cost/benefit analysis included?			
C.	Determine if the Feasibility Study or the formal project request for the new process contains all relevant information, including:			

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>	<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
<ul style="list-style-type: none"> <li>• Reasons for the project</li> <li>• Scope of the project</li> <li>• Constraints of the project</li> <li>• Costs and benefits of the project</li> <li>• Plans and schedules</li> <li>• User requirements</li> </ul>			
D. Review project administration activities for the following:			
1. Are periodic status meetings (Steering Committee) held?			
2. Do the Steering Committee meetings cover the following areas: <ul style="list-style-type: none"> <li>• Documenting project progress and highlighting variances from plan</li> <li>• Presenting revised plans</li> <li>• Budgetary control</li> <li>• Work status reporting and review</li> </ul>			
3. Are Action Items listed and Issues logged, maintained and reviewed during status meetings?			
4. Do the project team and management approve all extensions and deviations from plan?			
5. Are all-relevant parties notified of any plan changes in a timely manner?			
6. Has an acceptance procedure been defined and documented (e.g., formal acceptance/approval of major phases, and of the total project prior to production implementation)?			
7. Does everyone involved in the project understand their level of involvement, and their roles and responsibilities?			
8. Has a project change procedure been established (approval method, forms, cut-off dates, etc.)?			
9. Are original and newly identified risks documented, and are contingencies developed to address them?			

STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW

<u>Procedure</u>	<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
10. Do manual workarounds, needed to bridge missing functionality, include a staffing plan, a timeframe for termination, and projected volume capacity (how much work can we handle manually before we exhaust our capability to keep up timely)?			
<b>III. PROJECT PLAN – To determine if a comprehensive Project Plan has been developed</b>			
A. Are the critical phases determined?			
B. Does the plan require and identify management/user approval at specified points?			
C. Do the time lines appear realistic?			
D. Are GO/No-GO decision points identified and are they early enough in the project?			
E. For major tasks and milestones, does it identify- <ul style="list-style-type: none"> <li>• Start and end dates</li> <li>• Task duration</li> <li>• Prerequisites</li> <li>• Dependencies</li> <li>• Resource assignments</li> </ul>			
F. Are all major phases of project development identified, including – <ul style="list-style-type: none"> <li>• Testing phase(s)</li> <li>• User training in all areas, including reporting</li> <li>• Conversion</li> <li>• Implementation</li> </ul>			
G. Are all application areas included?			
H. Are all vendors identified and included?			
I. All interfaces to/from the application identified?			
<b>Section II – Infrastructure Integrity</b>			
<b>IV. Hardware / Technical Infrastructure - To determine if all required hardware components are in place prior to implementation</b>			
A. Determine if all required components have been identified, including computer (PCs, server, mid-range, etc.), printer, modems, telecom lines and equipment, etc.			
B. Review capacity planning documentation			

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
C.	Determine if there is a written plan and schedule for hardware installation. <ul style="list-style-type: none"> <li>Was the equipment ordered within the established project budget?</li> <li>Does the plan include an installation schedule?</li> <li>Does the plan appear reasonable?</li> <li>Will all components be installed prior to the scheduled implementation?</li> <li>Have contingency plans been developed for hardware replacement?</li> </ul>			
D.	Determine physical security measures for the technical infrastructure, including <ul style="list-style-type: none"> <li>Location of application/database servers</li> <li>Security of sensitive information workstations</li> <li>Printing of sensitive materials (i.e. HR, checks and PHI)</li> </ul>			
E.	Has data center facilities management considered the impact of the new hardware (e.g. physical space, connectivity, power, etc.)?			
<b>V. Data Security and Administrative Process – To determine if there is adequate security over application, data, transactions and database files.</b>				
A.	Determine network operating system controls to prevent unauthorized access to the system’s programs, files, databases and transactions.			
B.	Are both UserID and password required for access to the network?			
C.	Does the system lock out a UserID after a certain number if failed sign-on attempts?			
<b>VI. Determine who has the ability to issue/change passwords, and then review the control over user and password administration</b>				
A.	Considering separation of duties, is this an appropriate person?			
B.	Does the IT security department control the password assignments?			
C.	Are all user authorizations supported by a written or electronic approval from the data owner?			
<b>VII. Review the display and storage of network passwords.</b>				

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
A.	When typed or displayed on a screen or displayed on a report, are passwords masked/obliterated?			
B.	Are password files encrypted?			
C.	Are passwords stored in a visible (human readable) file?			
D.	Are passwords encrypted during transmission?			
<b>VIII.</b>	<b>Determine if all invalid/failed system access attempts are logged.</b>			
A.	Are all invalid network signon attempts captured?			
B.	Has management assigned an individual to review the invalid signon attempts?			
<b>IX.</b>	<b>SOFTWARE DEVELOPMENT LIFE CYCLE</b>			
A.	Define the development, testing and production environments. (should be distinct iterations)			
B.	Determine customized code migration process. <ul style="list-style-type: none"> <li>• Version control</li> <li>• Is access to migration tool limited?</li> </ul>			
C.	What documentation or library of customizations is maintained?			
D.	Are programmers prevented from normal access to production code and data?			
E.	Determine how unauthorized access to Production program libraries would be detected. <ul style="list-style-type: none"> <li>• Identify what is needed to gain access to Production program libraries. (Who has access to the Production libraries)</li> <li>• Identify what security monitoring exists on production program libraries</li> </ul>			
F.	Identify the procedures and controls for emergency program changes.			
G.	Determine how vendor-supplied changes to software packages are controlled and maintained			
H.	Ask the project manager if there are quality checks performed on modified software to ensure standards are followed, and documentation and testing are complete before moving the changes into production. If this is not a separate function and/or does not occur, make an audit comment.			

STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
I.	Confirm that programs are independently reviewed prior to implementation.			
<b>Section III – Application Controls</b>				
<b>X. Application Access Controls -</b>				
A.	Determine application controls to prevent unauthorized access to the system’s programs, files, databases and transactions			
B.	Are both UserID and password required for access to the application server?			
C.	Does the application lock out a UserID after a certain number if failed sign-on attempts?			
<b>XI. Compare transaction-level data security access levels to corresponding job assignments. Determine if access levels are adequate (just enough to perform job) and provide proper segregation.</b>				
A.	Are security access levels role-based, or individual-based?			
B.	Are there varying levels of security access (e.g., inquiry only, update non-monetary transactions, update financial transactions, add/delete records) for different types of transactions?			
C.	Are the levels appropriately assigned to the user department staff? Management and staff personnel who approve transactions should not have the authority to input or change the data			
D.	Who grants access to the application? And describe the processes regarding user administration (adding, changing or deleting users)			
E.	Determine if there are controls in place to prevent unauthorized access to the application’s source and object code.			
F.	Is access to the new system’s source and object code controlled by a software configuration management system providing strict and formal control over software copying, modification, and migration?			
<b>XII. Determine who has the ability to issue/change passwords, and then review the control over password administration</b>				

STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
A.	Who controls the passwords? Considering separation of duties, is this an appropriate person?			
B.	If password assignments are controlled by the user department, are 'password issuers' prohibited from having authority to input transactions?			
C.	Are all password authorizations supported by a written or electronic approval from the data owner?			
<b>XIII. Review the display and storage of application passwords.</b>				
A.	When typed or displayed on a screen or displayed on a report, are passwords masked/obliterated?			
B.	Are password files encrypted?			
C.	Are passwords stored in a visible (human readable) file?			
D.	Are passwords encrypted during transmission?			
<b>XIV. Determine if all invalid/failed system access attempts are logged.</b>				
A.	Are all invalid application signon attempts captured?			
B.	Has management assigned an individual to review the invalid signon attempts?			
<b>XV. Interfaces - To determine if there is adequate security and controls over interfaces to the new application.</b>				
A.	Identify the application interfaces with other systems. <ul style="list-style-type: none"> <li>Determine interface roll-out plan(s)</li> </ul>			
B.	Is an appropriate level of security wrapped around the interfaces?			
C.	Are the New Systems' interfaces properly documented?			
<b>Section IV – Testing and Data Conversions</b>				
<b>XVI. Testing - To determine if the test plan includes all aspects of the new system, the system is adequately tested prior to implementation, and all unexpected results are thoroughly resolved.</b>				
A.	Determine if the project team has developed a test plan.			
1.	Is the test plan written?			

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
2.	Does it include IS unit/functional testing, and user acceptance tests?			
3.	Are the users involved in developing the testing plan (e.g., producing test scripts or scenarios)?			
B.	Determine if all aspects of the system, as outlined in the detail Functional Specifications, will be tested, including, but not limited to: <ul style="list-style-type: none"> <li>• Data entry</li> <li>• Editing</li> <li>• Reports</li> <li>• Calculations</li> <li>• Error reporting</li> <li>• Interfaces with other systems</li> <li>• Network communications</li> <li>• Print handling</li> </ul>			
1.	Are all critical functions tested?			
2.	Are all existing capabilities tested?			
3.	Are all changes tested?			
4.	Will end-to-end system testing conducted prior to implementation?			
C.	Determine when testing will take place and ensure it will be completed prior to implementation.			
1.	Does the test plan allow for re-testing of errors and changes?			
D.	Determine if a parallel test will be run.			
1.	Have the criteria for the termination of the parallel run been identified? Note: parallel runs may continue until both systems are in sync			
2.	Does it include Information Systems and user acceptance/signoff?			
E.	Review month-end, quarter-end, and year-end tests.			

STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
F.	Determine if volume and/or stress testing will be done. <b>Note:</b> <i>Volume testing should include a “normal” processing day’s transactions as well as a high-volume day’s transactions, printing, backups, file transfers, interfaces, etc.</i> <b>Note:</b> <i>Stress testing should try to “overload” the system and provide an indication of maximum volume/thru-put the current configuration can be expected to handle. And, stress testing should test system response time in the stressed state.</i>			
<b>XVII. Test Procedures - To determine if adequate test procedures have been developed</b>				
A.	Determine if test data have been prepared			
B.	Does test data include all possible conditions, including errors?			
C.	Have test scripts been prepared?			
D.	Have the test files been defined?			
E.	Are the appropriate regions between test and production synchronized?			
F.	Have expected test results been defined prior to actual testing?			
G.	Do test scripts include all expected test results?			
H.	Have predetermined results been set up in advance (e.g., in a testing log)?			
I.	Have procedures been developed to monitor test results (e.g., in a log)?			
J.	Are the detail steps for the tests defined?			
K.	Are the controls over the application interfaces, e.g., access, balancing, data integrity, etc., included in the testing plan?			
<b>XVIII. Test Results - To determine if test results are consistent with expected results, and that unexpected results are monitored and addressed.</b>				
A.	Determine if procedures have been developed to evaluate the test results.			
1.	Are the users included in the testing process and evaluation of the results?			

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
2.	Are unexpected test results logged, monitored, and resolved?			
3.	Is there a problem resolution process for those tests not meeting the expected results? Note: Ask for a resolution-process flowchart.			
4.	Is the logging and problem resolution consistent with other implementations?			
<b>B.</b>	Review the test results and determine if unexpected results are handled properly.			
1.	Are unexpected test results evaluated to determine the reasons for the variance?			
2.	If needed, are program corrections made, or manual work arounds established?			
3.	Are the problems re-tested after correction?			
4.	Have all testing issues been resolved, or are work-arounds in place prior to implementation?			
<b>C.</b>	Follow those unexpected results deemed critical, to ensure adequate resolution. Determine if the tests having unexpected results were adequately re-tested after correction (to the program, etc.). All results that deviated from the expected should be re-tested.			
<b>XIX.</b>	<b>Data Conversion - To determine if the system conversion plans are adequate</b>			
<b>A.</b>	Obtain and review the conversion plan			
1.	Is the conversion plan written?			
2.	Is the data conversion approach defined?			
3.	Determine the type of conversion. Some conversion scenarios include: <ul style="list-style-type: none"> <li>• full conversion</li> <li>• “shell accounts” and update later</li> <li>• interim and “bridge” process</li> <li>• combination</li> </ul>			
4.	Has the conversion plan been approved by management and user departments?			
5.	Are all source systems identified?			

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
6.	Are all components identified (e.g., disks, tapes, telecom connections, etc.)?			
7.	Are the conversion rules and rationale documented?			
8.	Is a contingency plan defined?			
9.	Is a problem resolution scheme in place for the conversion phase?			
<b>B.</b>	<b>Separation of duties</b>			
1.	Are the appropriate IS and user operations staff available?			
2.	Is adequate separation of duties maintained during the conversion processes?			
<b>C.</b>	<b>Review the plans and procedures for balancing</b>			
1.	Are all needed files for the conversion identified?			
2.	Are all fields slated for conversion mapped to the new system?			
3.	Are there plans for verification of the data coming into the new system?			
4.	Are there procedures developed for balancing the number of records and totals for all monetary data elements and accounts for both the source files (before the conversion) and the resulting files (after the conversion)?			
5.	If so, are the procedures robust and adequate?			
6.	Are there before and after file compares planned, i.e., are the input files/records reconciled to the receiving files/records? Note: This should include all dollar fields, record counts and accounts.			
7.	Are appropriate edits and error reports in place to ensure data integrity?			
8.	Is a before and after conversion run planed to compare the old to new systems?			
9.	Determine if the rejects and errors will be re-entered and properly accounted for during the conversion.			

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>		<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
10.	Is there monitoring of all rejected transactions in the conversion?			
11.	Are these rejects researched and re-entered prior to cutover to the new system?			
12.	Are the errors/rejects considered as reconciling items when balancing?			
D.	Determine if there will be a parallel run after the actual conversion. Ensure that the results of the parallel run will be reviewed prior to the actual switchover to the new system.			
1.	Are run-to-run totals produced during parallel runs? Note: At the very least, after conversion, the new system should run the last day's processing so the results can be compared to the old system's.			
2.	Were the results of the parallel run consistent with expectations?			
E.	If a manual conversion, determine the procedures to verify all entries.			
<b>XX.</b>	<b>Final Acceptance/Approval of Conversion Process - To determine if criteria and procedures have been established for the new system's acceptance into the production environment</b>			
A.	Have standards for the final acceptance been established?			
B.	Are all stakeholders required to approve final acceptance of the tested system before the conversion can take place?			
C.	Has user department reviewed the system performance and operational test results, and approved the final results?			
D.	Have all problems encountered in the parallel run been resolved prior to full conversion?			
E.	After the conversion, was a sample of pre-selected records from the old system compared to the corresponding records on the new system?			
F.	Has the user and other stakeholder departments signed off on the conversion (accepted the conversion results) prior to discontinuing the old system?			

STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW

<u>Procedure</u>	<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
G. Was audit involved in the conversion?			
<b>Section V – Implementation Methodology</b>			
<b>XXI. Training - To determine if a training plan was developed for the project and if user training was adequate</b>			
A. Determine if a formal training plan was developed			
1. Does the training plan cover all aspects of the system, including: <ul style="list-style-type: none"> <li>• data entry</li> <li>• backups</li> <li>• management reporting</li> <li>• disaster recovery</li> <li>• user operations</li> <li>• computer operators</li> <li>• balancing and reconciliation</li> </ul>			
2. Does the training include vendor-recommended techniques?			
3. Did the training plan incorporate feedback from the users?			
B. Review the training plan to determine if training will be completed prior to implementation of the system			
1. Will the most critical employees be trained first?			
2. Will end-users be used to train others in lieu of a Training Department?			
3. Are differences between training environment and the production system taken into account during training?			
C. Determine who will be trained and at what level			
1. Will there be several levels of training: Management, data entry, supervisory?			
2. Will all appropriate levels of staff be trained?			
3. Will there be technical training for computer operators?			
4. Will there be report training? <ul style="list-style-type: none"> <li>• Report generation</li> <li>• Report design</li> </ul>			

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>	<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
<b>XXII. Back-out and Fall-back Plan – To determine if contingency plans regarding the implementation Go-Live are planned</b>			
A. Is there a problem resolution scheme in place for the installation phase?			
1. Will “help desk” personnel be available and adequately prepared			
2. Is the vendor and/or programmers available for problem resolution			
3. After installation and “shake-out” period, is the help desk ready and able to take over			
4. Do the users know where and how to obtain assistance			
B. Review the back-out/recovery plan.			
1. Does the back-out plan define when the back-out would be invoked?			
2. Does the back-out plan include procedures necessary to re-implement the old system, if needed?			
3. Does the back-out plan require approval from management prior to back-out implementation?			
4. Does the back-out include procedures for all affected areas?			
5. Does the back-out plan include a means to notify all areas/ users that the installation failed?			
<b>XXIII. Back-up &amp; Recovery – To determine if there are adequate back-up and recovery procedures are developed</b>			
A. Determine if there are documented procedures for regular system back-up, including operating systems, applications and data <ul style="list-style-type: none"> <li>• Development phase</li> <li>• After the system is placed in Production</li> </ul>			

**STANFORD UNIVERSITY  
IT INTERNAL AUDIT PROGRAM  
PROJECT DEVELOPMENT REVIEW**

<u>Procedure</u>	<u>Response</u>	<u>W/P Ref.</u>	<u>By</u>
1. Identify the following in back-up procedures: <ul style="list-style-type: none"> <li>• Back-up scheme</li> <li>• Frequency</li> <li>• Media</li> <li>• Where the back-up media be stored</li> <li>• Rotation</li> </ul>			
2. Do the back-up procedures include all foreseeable circumstances			
B. Are the recovery and restart procedures documented			
1. Do the recovery procedures include: <ul style="list-style-type: none"> <li>• Hardware and operating systems</li> <li>• User Workstations</li> <li>• Printers and print servers</li> <li>• Application software</li> </ul>			
C. Identify the retention period for the back-ups			
1. How long will the daily back-ups be kept?			
2. How long will month-end back-ups be retained?			
3. How long will quarter-end back-ups be retained?			
4. How long will year-end back-ups be retained?			
<b>XXIV. Disaster Recovery and Business Continuity</b>			
A. Determine if disaster recovery procedures have been developed			
1. While the system is in Development / Testing Phases			
2. After the system is in Production			
B. For critical business systems, is there a hot-site contract and testing schedule			
1. Is the hardware and supporting equipment for the new system included in the hot-site contract?			
2. Will the new system be scheduled for recovery testing in the next hot-site test?			
<b>XXV. CONCLUSIONS</b>			