

INTERNAL AUDIT WORKING PAPERS
2002 IT Change Management Policy

RISKS	RISK CLASSIFI - CATION & REF	RISK & RATIONALE	CONTROL POINTS	TESTS	RESULTS (Refer to test lead)	CONTROL RATING & CONCLUSIONS	TEST REF
Objective #1: To ensure a formally documented change management process exists and is maintained to reflect the current process.							
1. Lack of formal change management policies and processes could result in the delivery of inconsistent and unreliable products.	12 – Information Technology Risk	High I= Extreme, P= Moderate	1.1 Change management policies are formally documented.	1.1 Determine if existing change management policies have been formally documented.			
			1.2 The change management process is formally documented and kept updated.	1.2 Determine if change management processes have been formally documented. Determine if change management documentation has been kept up to date.			
2. Lack of awareness of change management policies and procedures may result in noncompliance. This may also lead to changes not being put through the corporate change management process.	12 – Information Technology Risk	High I= High, P= Likely	2.1 Management is responsible for promoting individual employee awareness of, and compliance with, corporate change management policies and procedures.	2.1 Determine if a process is in place to ensure that all current and new employees are informed of change management policies and procedures. Determine if employees are aware of relevant change management policies and procedures. Interview a sample of employees to determine if they have a clear understanding of their role and responsibilities.			

INTERNAL AUDIT WORKING PAPERS
2002 IT Change Management Policy

RISKS	RISK CLASSIFI - CATION & REF	RISK & RATIONALE	CONTROL POINTS	TESTS	RESULTS (Refer to test lead)	CONTROL RATING & CONCLUSIONS	TEST REF
Objective #2: To ensure change requests are properly initiated and approved.							
3. Unauthorized changes could result in unpredictable business solutions that would not meet the users' requirements. They may also adversely affect the production environment and result in increased costs.	12 – Information Technology Risk	High I= High, P= Likely	3.1 A process is in place to ensure that all changes are reviewed and approved by appropriate personnel before being introduced into the production environment.	3.1 Determine if process is in place to ensure that all changes are reviewed and approved by appropriate personnel. Obtain documentation supporting the approval process for a sample of changes.			
4. Lack of a priority assignment process for changes may result in the delay of critical change implementations.	12 – Information Technology Risk	High I= High, P= Likely	4.1 Change requests undergo a priority assignment process.	4.1 Determine if priorities are assigned to the change requests.			

INTERNAL AUDIT WORKING PAPERS
2002 IT Change Management Policy

RISKS	RISK CLASSIFI - CATION & REF	RISK & RATIONALE	CONTROL POINTS	TESTS	RESULTS (Refer to test lead)	CONTROL RATING & CONCLUSIONS	TEST REF
Objective #3: To ensure changes made to applications/systems are adequately tested before being placed into a production environment.							
5. Changes have not been tested before being implemented.	12 – Information Technology Risk	Significant I= High, P= Moderate	5.1 All changes are tested before being implemented in the production environment.	5.1 Determine if there is a process in place to ensure that changes have been tested prior to implementation. The testing/QA region should be separate from development and production. Obtain documentation stating changes have been received and reviewed by a QA type function for the selected sample of changes.			
6. The backout processes for changes have not been developed and tested prior to implementation.	12 – Information Technology Risk	High I= High, P= Likely	6.1 A backout process is developed and tested before any change request is implemented.	6.1 Determine if there is a process in place to ensure that backout procedures for changes have been developed and tested prior to implementation. Obtain documentation supporting backout processes for the selected sample of changes.			
7. Verification plans for implemented changes have not been developed and executed. Changes need to be verified to ensure they perform as expected.	12 – Information Technology Risk	High I= High, P= Likely	7.1 All change requests have a verification plan developed prior to implementation. Once implemented, change requests need to have documented verification results.	7.1 Determine if there is a process in place to ensure that verification plans for changes have been developed prior to implementation. Change verifiers need to execute the verification plan and document the results in the change requests. Obtain documentation supporting verification plans and results for the selected sample of changes.			

INTERNAL AUDIT WORKING PAPERS
2002 IT Change Management Policy

RISKS	RISK CLASSIFI - CATION & REF	RISK & RATIONALE	CONTROL POINTS	TESTS	RESULTS (Refer to test lead)	CONTROL RATING & CONCLUSIONS	TEST REF
Objective #4: To ensure all changes are being tracked adequately.							
8. Lack of a tracking process for changes being made to the production environment.	12 – Information Technology Risk	Severe I= Severe, P= Likely	8.1 There is a tracking process in place to ensure that changes to the production environment are documented and tracked throughout their lifecycle.	8.1 Determine if there is a process and/or change management tool in place to track changes throughout their lifecycle. Determine if there is adequate documentation for a sample of changes that have been implemented.			
9. Lack of monitoring of change requests may prevent changes that have not followed the change management process from being detected.	12 – Information Technology Risk	High I= High, P= Likely	9.1 A monitoring process is in place to ensure the change management process is working as intended.	9.1 Determine if a monitoring process is in place. Monitoring should include periodically reviewing changes made to the production environment to determine if any did not follow the change management process.			
Objective #5: To ensure all changes are adequately reported to stakeholders.							
10. Lack of reporting to stakeholders for all scheduled and completed changes may result in confusion and delays. This may adversely affect the production environment.	12 – Information Technology Risk	High I= High, P= Likely	10.1 All stakeholders are informed of changes once they have been scheduled as well as after they have been completed.	10.1 Determine if there is a process, such as automatic status notifications, in place to inform all stakeholders of changes that been scheduled as well as changes that have been completed.			

INTERNAL AUDIT WORKING PAPERS
2002 IT Change Management Policy

RISKS	RISK CLASSIFI - CATION & REF	RISK & RATIONALE	CONTROL POINTS	TESTS	RESULTS (Refer to test lead)	CONTROL RATING & CONCLUSIONS	TEST REF
Objective #6: To ensure all emergency changes are adequately managed and tracked.							
11. Lack of a formal change management process for emergency changes could result in unauthorized changes that may adversely affect the production environment.	12 – Information Technology Risk	Severe I= Extreme, P= Likely	11.1 The change management process for emergency situations is formally documented and kept updated.	11.1 Determine if change management processes for emergency changes have been formally documented. Determine if change management documentation has been kept up to date.			
12. Lack of post-review sessions for emergency changes may lead to repeating the same mistakes that lead to those changes.	12 – Information Technology Risk	Significant I= Medium, P= Likely	12.1 Post-reviews are conducted for all emergency changes so that factors that lead to the emergency changes may be reviewed and an impact assessment may be performed. This helps prevent the repetition of similar mistakes.	12.1 Determine if Change Management has documentation supporting a post-review process for a sample of emergency changes.			