Tool 5

Procedure voor een software-audit

Ontwikkeldatum:	8 mei 2003
Ontwikkeld door:	Van Bussel Document Services V.O.F.
Status:	versie 3.7.
Versiedatum:	4 januari 2006
Verspreiding:	Vrij te gebruiken met vermelding van copyright
Copyright:	Van Bussel Document Services V.O.F.
Taal:	Engels
Korte introductie:	Een diepgaande software-audit wordt slechts sporadisch uitgevoerd, zo merken wij in onze praktijk regelmatig. In 2003 hebben wij daartoe een procedure uitgewerkt om deze audits op een gestructureerde manier uit te voeren. Zeker met de steeds grotere nadruk op compliance is het toetsen van applicaties op hun werking een belangrijker. Ook voor document- en records managementapplicaties is (gezien hun bedrijfskritische betekenis) een periodieke audit noodzakelijk.

De procedure

PRELIMINARY AUDIT	
1.	Ascertain whether a prior audit has been performed. Obtain prior workpapers and determine what information can be pulled forward for the current audit.
2.	If a prior audit has been performed, obtain a copy of the audit report. For each audit issue/finding/control weakness, perform the following steps: a. Obtain and document the current status of each audit issue (include the name of the individuals you met, date of the interviews, and status of each issue). b. Note the disposition of each issue (Corrected/Still Open). c. If the issue still exists, carry it forward to the current audit report. Note in the follow-up workpaper that it was brought forward into the current audit report.
3.	Request the following documentation from the application and operational managers: • List of staff and their responsibilities for maintaining the application. • List of Business Units that utilize functions or output of the application. • Organization Charts from both the business units that utilize the system and the staff. • List of Major Changes made to this application since the last time audited. • List of Major Changes planned to be made to this application over the next 12 months. • Copy of the Application System User and Security Manuals. • Copy of the System Documentation relating to this application. • Vendor Contracts • Copy of the User Security Administration procedures for this application. • Service Level Agreement. • Contingency/Disaster Recovery Plans for this application. • Backup, Restart and Recovery Plan from Computer Operations.
4.	Interview the application and business unit owners to gain an understanding of how the application operates and identify any critical control points, including: a. Key concerns relating to this application system b. Owner roles in defining, prioritizing, testing and approving system changes c. Participation on key system projects Prepare a brief narrative to document your understanding.

5.	Review the Vendor contract supporting the application, ensuring that the following areas are addressed: a. Company Responsibilities b. Vendor Responsibilities c. Ownership and location of the application/source code. d. Release/upgrade testing and installation responsibilities. e. Maintenance agreements and terms f. If accessing our data, privacy clauses. Document the inclusion of the contract in the central Contract Management Database.

APPLICATION CONTROLS	
6.	Review system documentation obtained from the Preliminary Audit Steps to verify that it contains a description of: a. Transaction types processed b. System interfaces c. Critical program names and processing functions d. Batch job schedule (tasks) and critical processing performed e. Security Administration and access control procedures
7.	Obtain from the Preliminary Audit Steps or develop an overview system flowchart/narrative showing major input sources (e.g., system names/file names) and output types (e.g., report names/system names/file names/business user areas/IT areas).
	INPUT CONTROLS
8.	Obtain from the Preliminary Audit Steps or develop a flow of critical online input transactions. Identify the screen names and function types where the transactions are processed.
9.	Describe the edit and validation controls for critical input transactions. Review input screens to see that they are designed to prevent the omission of data and the acceptance of invalid data. Ensure that significant input is verified by an associate other than the person inputting the data.
10.	If the application uses batch processing, determine through test and observation that controls over input are effective.
	PROCESSING CONTROLS
11.	Review system documentation to determine that key computations are fully documented. Test a sample of key computations using a manual recalculation process.
12.	Determine and document the process to ensure that rejected transactions are corrected and re-entered promptly, and that corrected transactions are subject to the same edit and balancing controls as the original transactions.
13.	Determine that rejected items are logged, tracked, aged, and resolved timely. Review reject items reports to determine that: a. Reports are produced and distributed to the business user area. b. Reports evidence that they are reviewed daily by appropriate business user staff (e.g., user initials and review date). c. Rejects are resolved accurately and timely (e.g., request reject follow-up procedures).
	OUTPUT CONTROLS
14.	Verify that controls are in place to ensure that output confidentiality is maintained (when necessary). Obtain a list of reports indicating their frequency, purpose, and the identity of the recipient.
15.	Review reports produced by the application. Provide an opinion on the adequacy of the reports to satisfy the requirements of management. These requirements should have been gathered in the Preliminary Audit Steps.
16.	Determine that a review of critical transactions is performed. This should be performed by someone other than the person who input data from the source documents.

LOGICAL ACCESS CONTROLS	
17.	Review the User Security Administrator Procedures to ensure that: a. Procedures are in place for issuing, approving and monitoring application access.

	b. Application access procedures comply with the policy of "minimum access". c. User access control reports are periodically reviewed for accuracy and completeness by user management.
18.	Ensure that User Security Administration procedures are defined for the timely deletion/disabling of user Ids (e.g., hires, terminations, changes in responsibility).
19.	Verify that User Security Administration procedures exist to ensure that unique user Ids are assigned to system users. In cases where the access control system prevents individual accountability, compensating controls must exist.
20.	Obtain a sample of access request forms for 10 users of the application. Ensure that the forms evidence proper approvals for the requested access.
21.	Obtain a copy of the system generated user access report that identifies all users and their assigned authority levels and determine that: a. Only current employees have access to the application. b. All users are uniquely identified on the access control report. c. Passwords are not displayed on the report. d. Each user is granted an access level that is commensurate with their job responsibility. e. Management periodically reviews and approves users who have access to the application.
22.	Obtain a copy of the current Password Management/Access Control Policy and determine that this application complies with guidelines for: 1. Character components 2. Length 3. Password change frequency 4. Invalid password attempts 5. Password storage
23.	Obtain a job description for the Application Security Administrator function. Ensure that the reporting lines and responsibilities for this function do not compromise security policies.
24.	Identify the other responsibilities assigned to data security-related personnel besides security administration. Evaluate if a separation of duties deficiency may exist.
25.	Determine whether there are designated back-up security administrators. Ensure that the responsibilities of the back-up security administrators do not cause separation of duties deficiencies.
26.	Obtain copies of the security violation reports and verify that they evidence documented management review. Verify that questionable activity can be identified and is appropriately addressed.
27.	Determine that a review of the security administrator's maintenance activity is periodically performed by someone other than the User Security Administrator who performed the maintenance.

PHYSICAL ACCESS CONTROLS	
28.	Determine that access to sensitive application processing areas is adequately controlled. Document the physical access controls observed and tested.
29.	Verify that critical hardware (e.g., application servers) is protected from unauthorized access. Document the physical access controls observed and tested.

PROBLEM TRACKING AND MANAGEMENT PROCEDURES	
30.	Determine the processes used for problem resolution. Verify that information regarding problems is documented and retained whenever problems are encountered.

CONTINGENCY PLANNING AND BACK-UP	
31.	Obtain a copy of the business contingency and disaster recovery plans for the application. Review and evaluate the level of detail documented in the plan. Conclude on whether the plan appears effective in the event it would be relied upon in a disaster.
32.	Document the last time this application was Disaster Recovery tested. Verify the results of the test.
33.	Determine that copies of the contingency/disaster recovery plan and restart/recovery procedures are stored off-site.

SERVICE LEVEL AGREEMENTS	
34.	Obtain a copy of any Service Level Agreement related to this application.
35.	Interview users and determine whether the SLA requirements are being met such as: a. Timeliness of the information provided b. Accuracy of the information provided c. Names of IT contact people for problem resolution
36.	Determine if there is a process to identify and provide continual improvements to the application.
37.	Interview users and determine if they are aware of the application's processing capabilities in order to address current and future business needs. Verify that business user management informs IT about any future business strategies that will impact the application's processing requirements.