

**Company Name**  
**Audit Program**  
**JDE General IT Controls & Accounts Payables Review**

| <b>Step</b>                               | <b>Description</b>   | <b>Auditor/Ref.</b> |
|---|--|---------------------|
| <b><u>PURPOSE:</u></b>                    |  |                     |
|   | TBD  |                     |
| <b><u>SCOPE:</u></b>                      |  |                     |
|   | General computer controls specific to JDE and JDE Accounts Payable controls. |                     |
| <b>A. AUDIT PREPARATION AND REPORTING</b> |  |                     |
| 1.  | Control Log.   | _____               |
| 2.  | Final audit report.  | _____               |
| 3.  | Draft audit report(s).   | _____               |
| 4.  | Work Paper Review Notes.   | _____               |
| 5.  | Closing Conference Minutes.  | _____               |
| 6.  | Closing Conference Agenda.   | _____               |
| 7.  | Discussion Document - Closing Conference.                                    | _____               |
| 8.  | Opening Conference Minutes.  | _____               |
| 9.  | Opening Conference Agenda.   | _____               |
| 10.                                       | Audit Notification Letter.   | _____               |
| 11.                                       | Disposition of Prior Audit Findings.   | _____               |
| 12.                                       | Miscellaneous Financial, Operational and Background Data.                    | _____               |
| 13.                                       | Audit program.   | _____               |

**Company Name**  
**Audit Program**  
**JDE General IT Controls & Accounts Payables Review**

| <b>Step</b>                             | <b>Description</b>   | <b>Auditor/Ref.</b> |
|---|--|---------------------|
| <b>B. JDE ACCOUNTS PAYABLE CONTROLS</b> |  |                     |
| 1.                                      | <p>When you enter a document, such as an invoice or journal entry, you can assign a document number or let the Next Numbers program assign one. Next Numbers assigns numbers to documents using either or both of the following methods:</p> <ul style="list-style-type: none"><li>• <u>Standard next numbers</u>. The system finds the next available number in the Next Numbers table (F0002) and assigns the number to the document.</li><li>• <u>Next numbers by company and fiscal year</u>. The system assigns a unique set of next numbers for each company, fiscal year, or combination of company and fiscal year in the Next Numbers by Company/Fiscal Year table (F00021). From the General Systems menu (G00), choose Next Numbers. You can review the next numbers that the system assigns to journal entries and other documents.</li></ul>  |                     |
| 2.                                      | <p>Inquire as to whether management is generating and reviewing the budget comparison. (From the Non-Stock Purchasing menu (G43B), choose Purchasing Inquiries. From the Purchasing Inquiries menu (G43B112), choose Budget Comparison.)</p>   |                     |
| 3.                                      | <p>Perform inquiries to ensure management is utilizing standard JD Edwards or custom reports to verify receipts.</p>   |                     |
| 4.                                      | <p>Review a sample of invoices to ensure supporting documentation is provided and retained for an appropriate period.</p>  |                     |
| 5.                                      | <p>Verify that management generates, reviews, and follows up on exception reports.</p>   |                     |
| 6.                                      | <p>The A/P Original Document to G/L by Batch report verifies that the gross amount of each batch in the A/P Ledger table (F0411) is in balance with the amounts in the corresponding batch in the Account Ledger table (F0911). It also checks for an invalid pay status on every pay item. This report does not include batches of payments entered without voucher match (batch type W). To test the integrity of this type of batch, run the A/P Payments to G/L by Batch report. The A/P Payments to G/L by Batch report verifies that each batch of A/P Matching Document Detail (F0414) payments is in balance with the corresponding batch of Account Ledger (F0911) amounts. This test performs the following comparisons for each batch:</p> <ul style="list-style-type: none"><li>• Compares the gross amount in the A/P Matching Document Detail table to the gross amount in the Account Ledger table</li><li>• Compares the automatic offset amount to the A/P control amount</li><li>• Compares both of the above A/P and G/L amounts</li></ul> <p>The A/P to G/L by Offset Account report compares the open A/P Ledger (F0411) amounts to the balance in the offsetting A/P control (trade) accounts in the Account Balances table (F0902).</p> |                     |
| 7.                                      | <p>From the Accounts Receivable Setup menu (G03B41), choose Accounts Receivable Constants. Verify the fields for A/R Controls are established for all companies. Batch control option should be checked.</p>   |                     |

**Company Name**  
**Audit Program**  
**JDE General IT Controls & Accounts Payables Review**

| Step | Description  | Auditor/Ref. |
|------|--|--------------|
| 8.   | Conduct inquiries with management as to the numbering process for goods receipt vouchers.  |              |
| 9.   | In the security workbench, inquire on R09801, and P0011 to identify groups with ability to post. Identify users belonging to the groups in P0092 (user profiles) and cross reference listing with HR listing with job titles and/or discuss inappropriate access with Purchasing management.                           |              |
| 10.  | Interview management to determine goods returned note procedures.  |              |
| 11.  | From the Accounts Payable Setup menu (G0441), choose Accounts Payable Constants. On Accounts Payable Constants, verify that the Batch Control Required option is checked.  |              |
| 12.  | From the Accounts Payable Reports menu (G0414), choose the Suspected Duplicate Payments report. Also, verify that A/P constants have been set to identify duplicates (G0441).  |              |
| 13.  | Obtain and review JD Edwards reports for a sample month: <ul style="list-style-type: none"> <li>• Proof report</li> <li>• Bank Reconciliation report</li> <li>• Cleared Not Issued report</li> <li>• Cleared Before Issued report</li> <li>• Amounts Not Equal report</li> <li>• Un-reconciled Items report</li> </ul> |              |

**C. GENERAL JDE COMPUTER CONTROLS**

1. Users' initial menu on entry into JDE: Determine the organization's procedures for specifying users' initial menu on entry in JDE. Review a sample of users' profiles to assess whether this is specified appropriately. **Note**: The "initial menu/program" entry in the JDE user profile indicates the menu/program presented to the user on start up. This allows a user to be restricted to a specific application such as Fixed Assets. **Risk**: Users may be able to access sensitive system commands or other options which are not otherwise restricted.
  
2. Accounting constants: Review the General Accounting, Accounts Payable and Accounts Receivable Constants that have a key impact on the control environment. **Note**: Accounting constants are used to specify how the Accounting modules function and how available controls are used within individual JD Edwards environments. A number of the settings have a pervasive effect and so have a major impact on the control environment. The constants are only configured once during the implementation process. Once these settings are established, it should not be necessary to change them.
  - Management Approval of Input:
  - Prior Accounting Period Posting
  - Allow Posting to Invalid Accounts
  - Settlement of Intercompany Balances

**Company Name**  
**Audit Program**  
**JDE General IT Controls & Accounts Payables Review**

| Step | Description  | Auditor/Ref. |
|------|--|--------------|
|      | <ul style="list-style-type: none"> <li>• Post Out of Balance Journals</li> <li>• Multi-currency conversion</li> <li>• Batch Control Required</li> <li>• Duplicate Invoice Number Edit</li> <li>• General Ledger Interface</li> </ul>   |              |
| 3.   | <u>Management Approval of Input</u> : It is recommended that this is set to "Y" to affect segregation of duties. An "N" indicates that batches will automatically default to a status of "approved".   |              |
| 4.   | <u>Prior Accounting Period Posting</u> : It is recommended that this constant is set to "N". A "Y" allows journals to be entered to prior accounting periods and raises the risk that the integrity of past financial data could be compromised.   |              |
| 5.   | <u>Allow Posting to Invalid Accounts</u> : It is recommended that this flag is set to "N". "Y" settings would allow postings to be made to accounts, which have not yet been set-up on the Chart of Accounts Master file.  |              |
| 6.   | <u>Settlement of Intercompany Balances</u> : A "*" indicates that intercompany transactions will not be created but the batch will post anyway resulting in the accounts being out-of-balance. It is recommended that "*" is never used. The other flags can be used depending on the conditions involved. |              |
| 7.   | <u>Post Out of Balance Journals</u> : It is recommended that this flag be set to "N".  |              |
| 8.   | <u>Multi-currency conversion</u> : The flags set will depend upon management's procedures for currency conversion.   |              |
| 9.   | <u>Batch Control Required</u> : An "N" bypasses the batch header screen. It is recommended that this flag be set to "Y".   |              |
| 10.  | <u>Duplicate Invoice Number Edit</u> : "Y" or "H" is recommended settings since a "N" disables this feature.   |              |
| 11.  | <u>General Ledger Interface</u> : Postings will not be made automatically to the General Accounting module if this is set to "N".  |              |

**D. USER'S ACCESS TO THE COMMAND LINE**

1. Assess whether users gain access to the command line by reviewing settings of "allow command entry" flag in the JDE user profile and the "limit capabilities" flag in the OS/400 flag in the OS/400 user profile. Ensure that the "allow command entry" flag in the JDE user profile is set to "N", and that the "limit capabilities" flag in the OS/400 user profile is set to "YES". **Note:** Users' access to the operating system command line is controlled by two parameters: The "Allow Command Entry" flag in the JD Edwards user profile. This can either be set to "Y"-Yes, or "N"-No. If this is set to "N", then the user does not have access to the command line and the setting negates the risk of a user

**Company Name**  
**Audit Program**  
**JDE General IT Controls & Accounts Payables Review**

| Step | Description | Auditor/Ref. |
|------|-------------|--------------|
|------|-------------|--------------|

breaking free from JD Edwards' restrictive menu systems. It is recommended that this flag is set to "N". The "Limit Capabilities" flag in the OS/400 user profile. If this is set to "\*YES", users are restricted from access to the operating system command line. It is recommended that this flag is set to "YES". These two commands must be used in conjunction with each other. The command line setting in the JD Edwards user profile overrides that on the OS/400. For example, if the "Allow Command Entry" flag in JDE is set to "Y", and the "Limit Capabilities" flag in OS/400 is set to "\*YES", the user will have access to the command line.

2. Users' access to menus: Determine the organization's procedures for allowing users to menu travel. Review a sample of users' profiles to assess whether this flag has been set to "N" to prevent menu traveling. Assess the implications if flags have been set to "Y". **Note:** The Menu Traveling flag within a user's profile allows a user direct access to a menu even if the user cannot view the menu directly. This flag can either be set to "Y" or "N". If the menu traveling flag is set to "Y", users can type the number of the screen they wish to travel to and are then sent directly to it. For example users travel directly to the Security Officer menu by typing "A94". Access to menu traveling may negate other security settings by giving users the ability to circumvent security features offered by other menu restrictions.
  
3. Users' access to menu options-fast path: Determine the organization's procedures for allowing users to fast path. Review a sample of users' profiles to assess whether this flag has been set to "N" to prevent them being able to fast path. Assess the implications if flags have been set to "Y". **Note:** Each screen in JD Edwards has a unique number shown in the top left hand corner of the screen. The Fast Path flag within a user's profile allows the user to move directly to another screen within JD Edwards. This flag is either set to "Y", or "N". Access to fast pathing may negate other security settings by giving users the ability to circumvent security features offered by other menu restrictions.

**E. JDE USER PROFILE SECURITY**

User profile security within JDE is very flexible and can be very powerful. However the nature of the various independent but over-lapping security functions available is such that the set-up of the access security function must be a carefully planned and executed set of procedures to ensure that logical access paths are correctly defined.

1. Users' profiles-user keys and menu locks: Review the organization's procedures for defining user key and menu key security. Review a sample of user profiles to assess whether users can access sensitive menus or screens. **Note:** User Keys (defined in the JD Edwards user profile) and Menu Locks (defined for each JD Edwards menu and menu selection) are fundamental tools used for matching users to appropriate menus/menu selections. Each User Key and Menu Lock has a number of allocated values or settings. A user can only gain access to a menu or menu selection if their User Keys exactly match the Menu Lock for the Job ("J"), Department ("DP") and Future ("F") Codes, and match or exceed the Authority ("A") and Knowledge ("K") levels.

If no level / code is defined for a user key or menu lock then access is allowed by default. For example, even if a menu lock is set very restrictively (such as authorization level-1), if no

**Company Name**  
**Audit Program**  
**JDE General IT Controls & Accounts Payables Review**

| Step | Description  | Auditor/Ref. |
|------|--|--------------|
|      | <p>corresponding setting has been made in the user's user key, the user would gain access by default a sensitive menu or menu selection. Security officers can prevent access by default by specifying "X" in the allocated position.</p>  |              |
| 2.   | <p><u>Users' profiles-action code security</u>: Review the organization's procedures for defining action code security. Review a sample of user profiles and program ids to assess how action code security has been defined. Assess the security implications if user ids do not have action codes. Assess which users are able to inquire upon UDC restriction settings, and assess the security implications.<br/> <b>Note</b>: Action code security can be defined: By user ID with a list of programs that the user is denied or granted access to, or By program ID with a list of users denied or granted access to that program. For each program ID or user ID, the three action codes (add, change or delete) are defined by flagging "Y" or "N". If a user ID is not specifically defined as having an action code for a specified program ID then default access is to allow add, change and delete entry to that menu selection. To prevent this situation arising, the *PUBLIC ID can be used to specify default access. User Defined Codes (UDC) is implemented by key users who are allocated the appropriate Action Code to use this menu option (program ID). Any user with the ability to inquire on the UDC restriction settings can also add, change and delete these settings.</p> |              |
| 3.   | <p><u>Users' profiles-business unit/cost center security</u>: Business unit/cost center security can be specified by user ID or file ID. Review the organization's procedures for defining business unit / cost center security. Review a sample of user profiles and program ids to assess how this has been defined. Assess the security implications if user ids / file ids are incorrectly defined.</p>  |              |
| 4.   | <p><u>Users' profiles-batch approval/post security</u>: Review the organization's procedures for defining batch approval and post security to users. Review those users who are able to batch approve and post and assess whether these are appropriately defined. Assess whether users can input and approve batches. Assess the security implications if user ids are incorrectly defined. _JD Edwards can enforce authorization of all batches prior to any processing and posting. This control is initially set as follows:</p> <ol style="list-style-type: none"> <li>1. By identifying the modules in which this feature should operate (see "accounting constants"). Batch approval security can only be set up for General Accounting, Accounts Payable and Accounts Receivable modules.</li> <li>2. Specifying which users can authorize other users' batches. There are two sets of users: the "approved by" and "secured by" users.</li> <li>3. That inappropriate users are able to approve and post batches.</li> </ol>  |              |
| 5.   | <p><u>Users' profiles-function keys</u>: The user has access to a number of functions by use of "function keys" within each menu / menu selection on JD Edwards. Review the organization's procedures for defining batch approval and post security to users. Review option 7 of the main Security Officer menu-"Review User Security"-to identify which users have function key security specifically set.<br/> <b>Note</b>: Users can use function keys to access locations which are not on the menus they usually encounter, potentially short-cut any "masked" menu selections. Access to function keys may negate other security settings by giving users the ability to circumvent security features offered by other menu restrictions or over-ride key prevent controls. The availability of each function key to users (or users' access to a screen's specific function keys) is set to "Y" to allow access and "N" to</p>  |              |

**Company Name**  
**Audit Program**  
**JDE General IT Controls & Accounts Payables Review**

| Step | Description | Auditor/Ref. |
|------|-------------|--------------|
|------|-------------|--------------|

deny access. If the field is left blank, access to the function key is given by default. Due to the complexity of the control procedures required over function keys, Function Key Security is not normally used but, for the same reason, is one of the most difficult control risks to negate.

6. Users' profiles-name search security: Review the organization's procedures for defining name search security to users. Select a sample of users to identify which users have name search security specifically set. Name search type security is used to help secure Address Book records. Each constituent member of a key element of the Address Book such as banks ("B"), or vendors ("V"), has a prefix to denote where in the Address Book it is maintained. Name Search Type Security is based on these prefixes. Access to the Address Book, as the basis of a significant number of preventive controls as well as the main repository of information, needs to be appropriately restricted. For example, a member of the Accounts Payable department should be restricted from amending bank details.

**F. REPORT GENERATOR SECURITY**

1. Review the organization's procedures for defining report generator security. Select a sample of business critical reports to identify whether the security has been appropriately set. **Note:** Report Generator Security provides four different levels of access to report generating programs. Security levels must be set once a new report-generating program has been developed, and can be amended subsequently. If security levels are set to 0 or 1 they will be prone to unauthorized amendment. Level 3 (owner-only access) security can cause inefficiencies in that no other user is able to run a report-generating program.
2. Use of reports: Review the organization's procedures for control report use and access. Assess the adequacy of these procedures. **Note:** JD Edwards software has been produced to enable the user to act the part of the programmer (by producing the programs using the report generators), and the operator (by being able to run the interrogation when and where they want by manipulation of the job and print queues).
3. Users' access-currency codes: Select a sample of users with access to program P0013 and assess the adequacy of this access. **Note:** The program P0013 (option 3 from menu A113) is used to designate the currency codes and the number of decimal places used for currency conversion. If the decimal place setting is changed, the system will scan all previous transactions and change the amounts to reflect the new setting, and as such that access to menu A113 options and programs should be carefully controlled.
4. Users' access-master records: Sensitive details are held on the Master records such as for Customer and Vendor master files. Unauthorized amendments may be made to customer or vendor master files. Review the organization's procedures:
  - a. Access to the Address Book is restricted to specific members of staff to ensure control over sensitive information and the existence of segregation of duties.
  - b. All amendments to Address Book details have to be authorized by a relevant party.
  - c. Regular reviews of all changes to Address Book details are undertaken. For versions 5.2

**Company Name**  
**Audit Program**  
**JDE General IT Controls & Accounts Payables Review**

| <b>Step</b> | <b>Description</b>   | <b>Auditor/Ref.</b> |
|-------------|--|---------------------|
|             | <p>and prior, the only way to obtain this information is to use a WORLDwriter interrogation. JD Edwards has helped clients develop this program. A standard JD Edwards report in Version 6 and onwards containing this information is available.</p>   |                     |
| 5.          | <p><u>Appropriateness of AAI settings:</u> Review set up of AAIs to ensure appropriately set up. Assess extent to which AAIs are being used. Automatic accounting instructions (AAIs) are used to define the General Accounting module accounts modules such as Accounts Payable should post to. The General Ledger module may not be fully updated automatically due to AAIs being incorrectly set-up. This will lead to the accounts being out of balance.</p> |                     |