

Oracle Application Security & Controls

by
Ellen Chan & Yogita Parulekar

6th October, 2004

Oracle Application Security & Controls

- **Steps to design and conduct an audit of the automated controls of the Oracle application, their risks and impact on the input, processing, and output of financial information**
 - Define scope of audit
 - Understand organizational hierarchy in the Oracle application
 - Identify automated controls in the Oracle application & supplemental manual controls

Oracle Application Security & Controls

- **Define scope of audit**
 - **Objectives**
 - **Business cycle**
 - **Processing location**
 - *What applications?
Which modules?*
 - *Which “organizations”
or “operating units”?*

Oracle Application Security & Controls

- **Understand Organizational Hierarchy in Oracle application**
 - **Classifications**
 - **Set of books**
 - **Operating units**
 - **Inventory organizations**

Oracle Application Security & Controls

Set of Book

Define Organization
– Operating Unit information

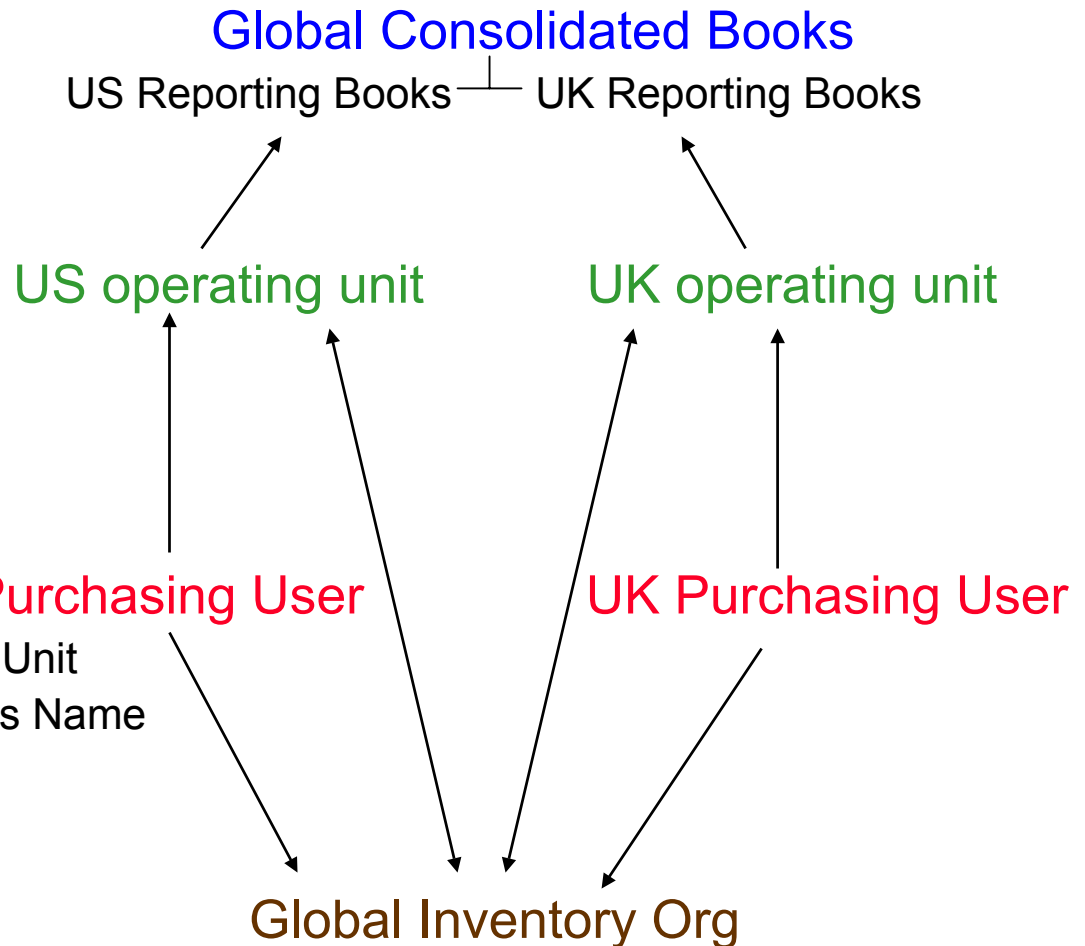
Operating Units

Striped setup:
e.g. Match Approval Level
(2,3, 4 way match)

Responsibilities

Profile option: MO: Operating Unit
Profile option: GL Set of Books Name

Inventory Organizations



Oracle Application Security & Controls

- **Why do we care?**
 - Segmentation of data to provide access security
 - Some setups are segmented (striped) by organization
 - These impact:
 - sample selection and sample size
 - access required for conducting the audit

Oracle Application Security & Controls

- Define scope of audit
- Understand organizational hierarchy in the Oracle application
- **Identify automated controls in the Oracle application & supplemental manual controls**

Oracle Application Security & Controls

- **Identify automated controls in the Oracle application & supplemental manual controls**
 - **Understand business process flow and risk**
 - **Identify & evaluate key controls**
 - **Source of controls, and their types**
 - **Manual**
 - **Combined (e.g. reports, alerts)**
 - **Automated – Inherit, Setup, Workflow/customized program, Access**
 - **Change control**

Oracle Application Security & Controls

Risk	Control Objective				Controls Activities	Who Performs	Control Type	Automation Type
	Compliance	Effectiveness/ Efficiency	Safeguarding	Reliability on Financial Statements				
					<div style="border: 1px solid black; background-color: #ffffcc; padding: 5px;"> Choices can be as follows · "C" for completeness or · "E" for existence or occurrence or · "P" for presentation and disclosure or · "O" for rights and obligations or · "M" for Measurement or valuation </div>			
Unauthorized invoices are processed for payment		X	X	C, M	Invoice that does not match to a Purchase Order will not be not processed without the appropriate approvals.	AP Analyst	Manual	N/A
		X		C, M	"Match Approval Level" is set to 3-way at the System Level as the default to ensure that purchase order, receipt, and invoice quantities must match within tolerance before the invoice can be paid.	Application: Payables	Automatic	Setup
		X		C, M	Any overrides of the "Match Approval Level" at the Item, Vendor, or Purchase Order level requires approval and is reviewed on a regular basis.	Purchasing Manager	Manual	N/A
		X		C, M	Matching tolerances are set to 0% for Quantity Ordered tolerance, 0% for the Quantity Received tolerance and 0% for the Price tolerance. If the transaction exceeds the designated tolerance level, the invoice will be placed on hold and will not be paid.	Applications: Payable	Automatic	Setup
		X		C, M	On a weekly basis, the "Invoice on Hold" report is generated and reviewed to detect invoices being released from holds without adequate approval.	AP Manager	Combination	Report

Oracle Application Security & Controls

- Ways to gather automated control information
 - Online review
 - Reports (limited, e.g. *Financials/Purchasing Options Listing, users of a responsibility*)
 - Export table on forms screen (File -> Export -> Save As)
 - Database scripts

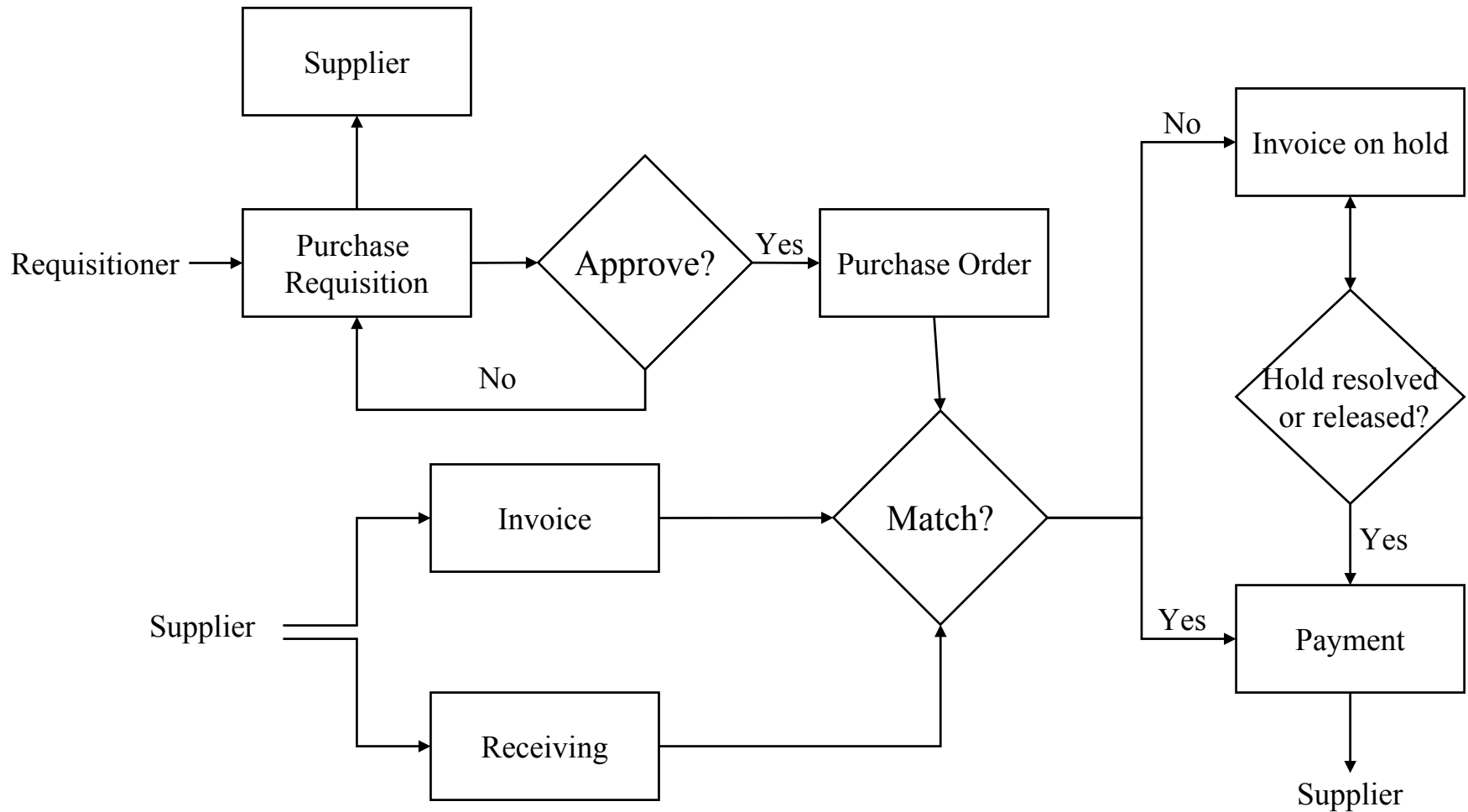
Oracle Application Security & Controls

- **Example - Procure to Pay for UK**
 - **Procurement: manual, custom requisition application, Oracle Purchasing**
 - **Invoicing & Payment: Oracle payables**
 - **Period-end Close: Oracle payables, general ledger**
 - **.....**

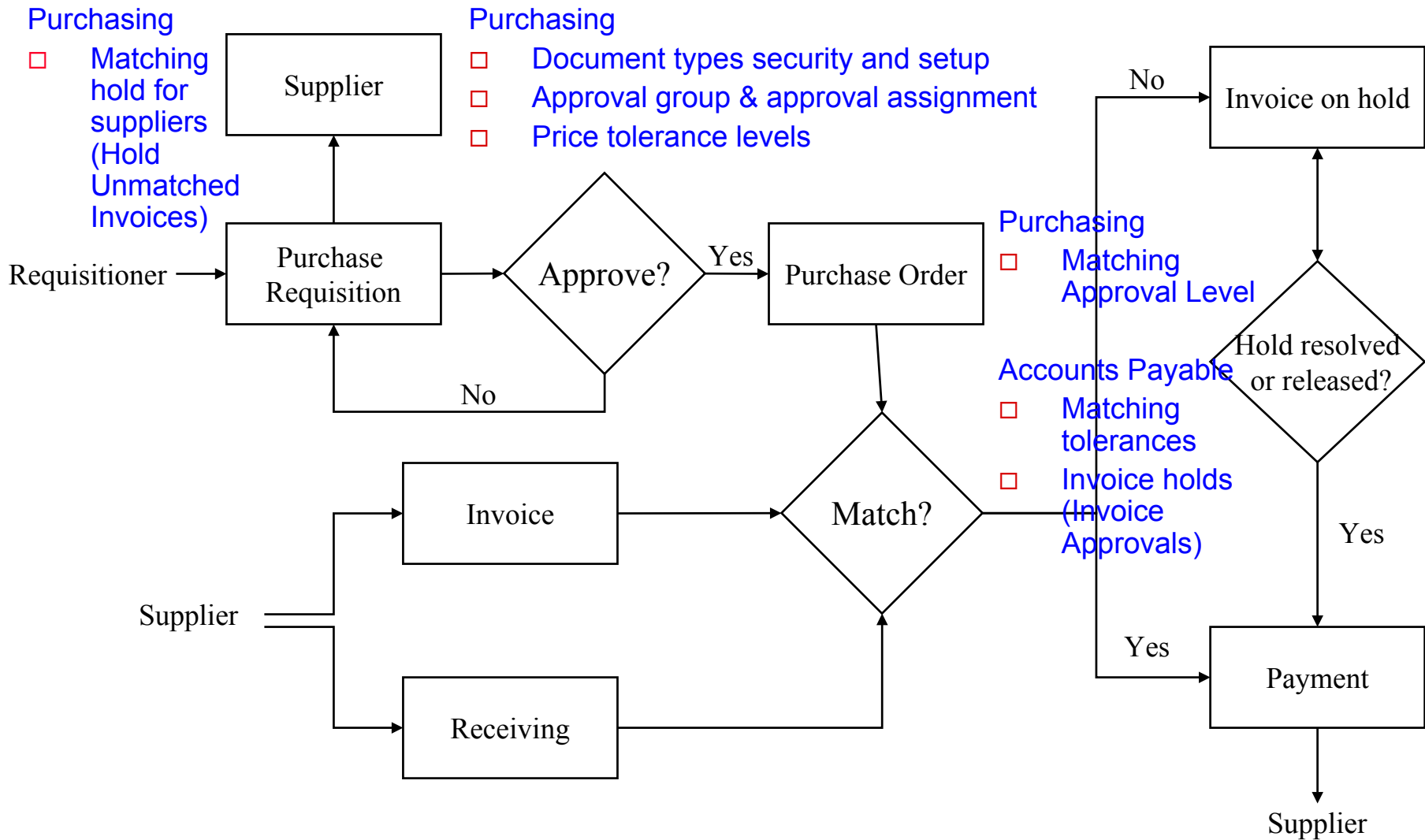
Oracle Application Security & Controls

- **Example - Procure to Pay for UK**
 - Procurement: manual, custom requisition application, Oracle Purchasing
 - Invoicing & Payment: Oracle payables
 - Period-end Close: Oracle payables, general ledger
 - etc.
 - Operating units
 - Set of books
 - Responsibility

Oracle Application Security & Controls



Oracle Application Security & Controls - Setup



Oracle Application Security & Controls - Setup

- Purchasing
 - Document types security and setup

The screenshot shows the 'Document Types (Vision Operations)' window. The 'Document' section contains a table with the following data:

Type	Subtype	Name	Quotation Class
Purchase Order	Standard	Standard Purchase Ord	

The 'Attributes' section contains the following settings:

- Owner Can Approve
- Approver Can Modify
- Can Change Forward-To
- Can Change Forward-From
- Can Change Approval Hierarchy
- Disable
- Security Level: **Public**
- Access Level: **Full**
- Forward Method: **Direct**
- Archive on: **Print**
- Default Hierarchy: **Materials**
- Approval Workflow: **PO Approval**
- Workflow Startup Process: **PO Approval Top Proce**
- Autocreate Workflow: [Empty]
- Autocreate Workflow Startup Process: [Empty]

Oracle Application Security & Controls - Setup

- Purchasing
 - Use Approval Hierarchies = Yes, approval paths based on position hierarchies (described in the next two slides)
 - Use Approval Hierarchies = No, approval paths based on supervisor structure.

The screenshot shows the Oracle Financials Options window with the 'Supplier - Purchasing' tab selected. The window contains several fields and a checkbox:

- Business Group:** [Empty text field]
- Expense Reimbursement Address:** [Home] (dropdown menu)
- Use Approval Hierarchies:** (checkbox, circled in red)
- Employee Number:** [Empty text field]
- Method:** [Automatic] (dropdown menu)
- Next Automatic Number:** [56903] (dropdown menu)

Oracle Application Security & Controls - Setup

- Purchasing
 - Approval group & approval assignment

Define approval group (dollar limit and account limit)

-> Assign to HR job by document type

Approval Groups (V1)

Name: **Buyer Materials** Enabled

Description: **Buyer for materials up to \$50,000**

Approval Rules

Object	Type	Amount Limit	Low Value	High Value
Document Total	Include	50,000.00		
Account Range	Include	50,000.00	01,000.0000.0000.000	02,999,9999.9999.999

Oracle Application Security & Controls - Setup

- Purchasing
 - Approval group & approval assignment

Define approval group (dollar limit and account limit)

-> Assign to HR job by document type

Assign Approval Groups (V1)

Position: 710.ADMIN ASSISTANT Organization: Vision Administration

Job: STA700.Staff Administrator

Approval Assignments

Document Type	Approval Group	Effective From	Effective To
Approve Standard Purchase	Buyer Materials	15/JAN/2001	

Oracle Application Security & Controls - Setup

- Purchasing
 - Price tolerance levels

The screenshot shows the 'Purchasing Options (Vision Operations)' window with the 'Control' tab selected. The 'Price Tolerance' is set to 10% and 'Enforce Price Tolerance' is checked. Other options include 'Enforce Full Lot Quantity' (Advisory), 'Receipt Close Point' (Delivered), 'Cancel Requisitions' (Optionally), 'Security Hierarchy' (Materials), 'Display Disposition Messages' (checked), 'Notify If Blanket PO Exists' (checked), 'Allow Item Description Update' (checked), 'Enforce Buyer Name' (unchecked), and 'Enforce Vendor Hcid' (checked).

Option	Value
Price Tolerance	10 %
Enforce Price Tolerance	<input checked="" type="checkbox"/>
Enforce Full Lot Quantity	Advisory
Receipt Close Point	Delivered
Cancel Requisitions	Optionally
Security Hierarchy	Materials
Display Disposition Messages	<input checked="" type="checkbox"/>
Notify If Blanket PO Exists	<input checked="" type="checkbox"/>
Allow Item Description Update	<input checked="" type="checkbox"/>
Enforce Buyer Name	<input type="checkbox"/>
Enforce Vendor Hcid	<input checked="" type="checkbox"/>

Oracle Application Security & Controls - Setup

- Purchasing
 - Matching Approval Levels
 - *Two-Way*: Purchase order and invoice quantities must match within tolerance before the corresponding invoice can be paid.
 - *Three-Way*: Purchase order, receipt, and invoice quantities must match within tolerance before the corresponding invoice can be paid.
 - *Four-Way*: Purchase order, receipt, inspection, and invoice quantities must match within tolerance before the corresponding invoice can be paid.

The screenshot displays the 'Purchasing Options (Vision Operations)' window with several tabs: Accrual, Control, Default, Internal Requisition, Numbering, and Tax Defaults. The 'Default' tab is active. The window contains the following fields and values:

Requisition Import Group-By	Item	Rate Type	Corporate
Minimum Release Amount	1.00	Price Type	
Price Break Type	Cumulative	RFQ Required	<input type="checkbox"/>
Quote Warning Delay	7	Receipt Close	10 %
Invoice Close	1 %	Line Type	Goods
Match Approval Level	3 Way		

The 'Match Approval Level' dropdown menu is circled in red, indicating the selected value is '3 Way'.

Oracle Application Security & Controls - Setup

- ❑ Purchasing/Accounts Payable
 - ❑ Matching hold for suppliers

The screenshot shows the Oracle Financials Options window with the 'Supplier - Purchasing' tab selected. The 'RFQ Only Site' checkbox is unchecked. The 'Hold Unmatched Invoices' checkbox is also unchecked and is circled in red. The 'Invoice Match Option' is set to 'Purchase Order'. The 'Supplier Number' section is expanded, showing 'Entry' set to 'Automatic', 'Type' set to 'Numeric', and 'Next Automatic Number' set to '194072'.

RFQ Only Site	<input type="checkbox"/>
Hold Unmatched Invoices	<input type="checkbox"/>
Invoice Match Option	Purchase Order
Supplier Number	
Entry	Automatic
Type	Numeric
Next Automatic Number	194072

Oracle Application Security & Controls - Setup

- Accounts Payable
 - Matching tolerances (Quantity Ordered/Received, Price)

The screenshot shows the 'Invoice Tolerances' window in Oracle. It is divided into two main sections: 'PO Matching' and 'Tax'.

PO Matching Section:

	Tolerance	Hold Name	
Quantity Ordered	1.0 %	Qty Ord	<input checked="" type="checkbox"/>
Maximum Quantity Ordered		Max Qty Ord	<input type="checkbox"/>
Quantity Received	1.0 %	Qty Rec	<input checked="" type="checkbox"/>
Maximum Quantity Received		Max Qty Rec	<input type="checkbox"/>
Price	5.0 %	Price	<input checked="" type="checkbox"/>
Exchange Rate Amount		Max Rate Amount	<input type="checkbox"/>
Shipment Amount		Max Ship Amount	<input type="checkbox"/>
Total Amount		Max Total Amount	<input type="checkbox"/>

Tax Section:

Tax		%	Tax Variance	<input type="checkbox"/>
Tax Amount Range			Tax Amount Range	<input type="checkbox"/>

Oracle Application Security & Controls - Setup

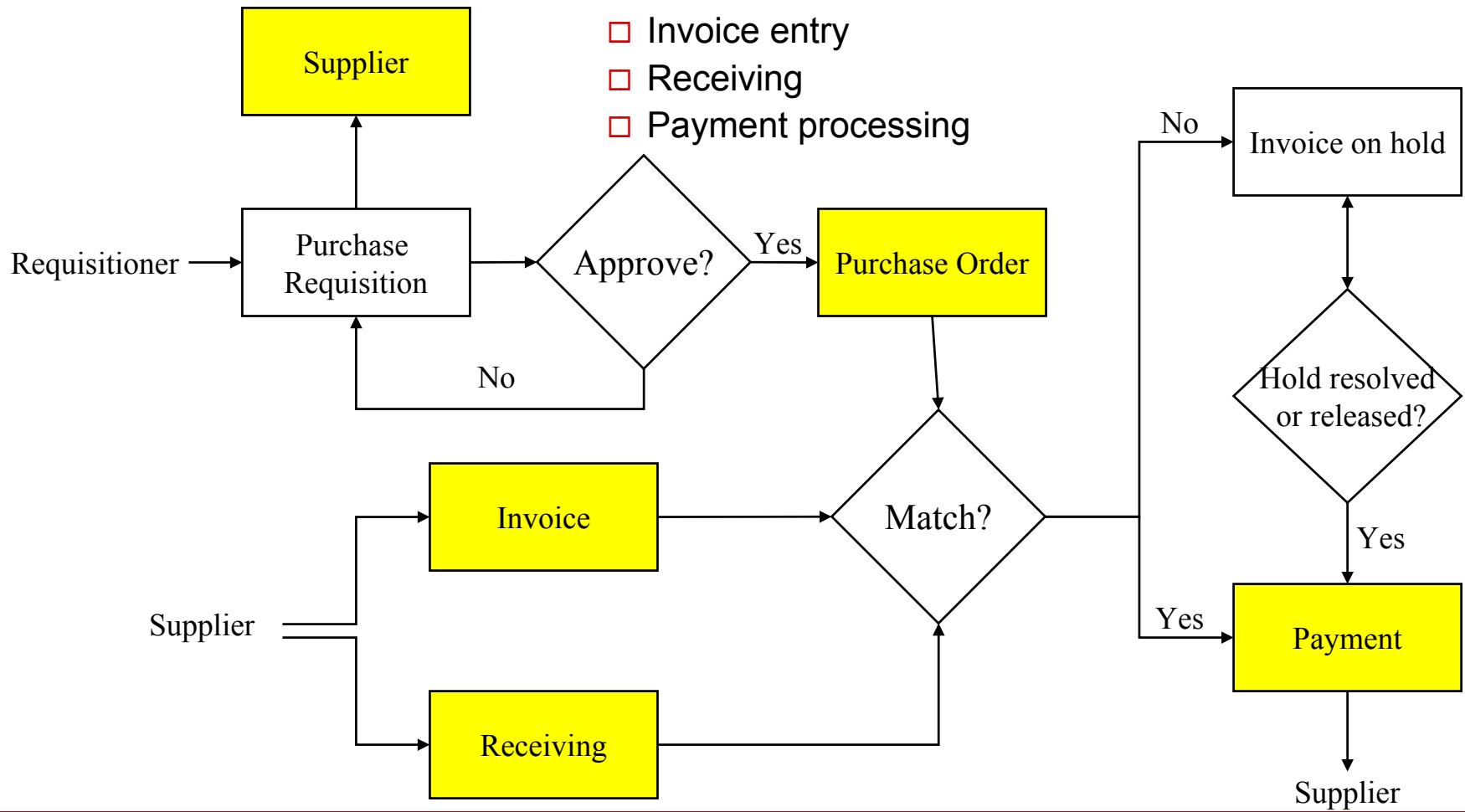
- Purchasing
 - Invoice holds (Invoice Approvals)

The screenshot shows a window titled "Invoice Hold and Release Names" with a table of hold reasons. The table has columns for Name, Description, Type, Accounting Allowed, Manual Release Allowed, and Inactive On. The first row, "Await Credit", has its "Accounting Allowed" and "Manual Release Allowed" checkboxes circled in red. The "Manual Release Allowed" checkbox is checked, while the "Accounting Allowed" checkbox is unchecked. The "Inactive On" column for this row is empty.

Name	Description	Type	Accounting Allowed	Manual Release Allowed	Inactive On
Await Credit	Await Credit	Invoice Hold Reason	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Awaiting Credit (Dave)	Invoice for which Credit is du	Invoice Hold Reason	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Awaiting Credit (Purch)	Invoice for which Credit is du	Invoice Hold Reason	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Awaiting Credit Note	Invoice awaiting credit note	Invoice Hold Reason	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	12-JAN-2000
Awt Acct Invalid	AWT Account is invalid	Acct Hold Reason	<input type="checkbox"/>	<input type="checkbox"/>	
Awt Acct Valid	AWT Account is now valid	Acct Release Reason	<input type="checkbox"/>	<input type="checkbox"/>	

Oracle Application Security & Controls - Access

- ❑ Basic segregation of duties
 - ❑ Suppliers
 - ❑ Purchase order creation
 - ❑ Invoice entry
 - ❑ Receiving
 - ❑ Payment processing



Oracle Application Security & Controls – Access

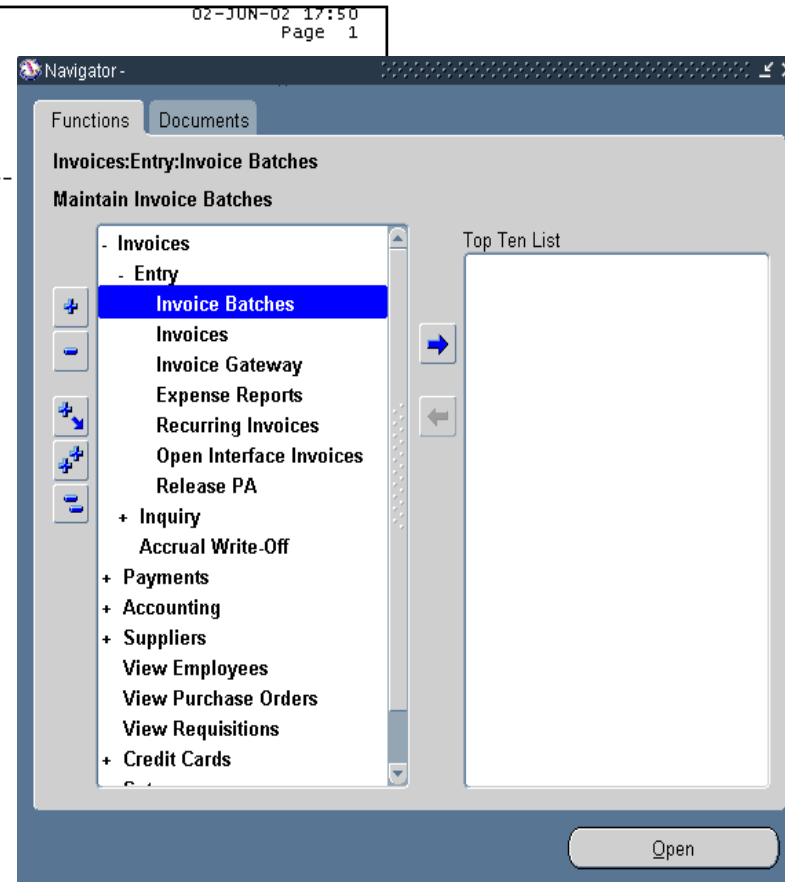
- Steps and Methods
 - Audit for incompatible access within each responsibility
 - Function Security Menu report**
 - Main Menu
 - Sub Menu 1
 - Function A
 - Function B
 - Sub Menu 2
 - Function C
 -
 - Function exclusions
 - Audit for incompatible access for a user by granting multiple incompatible responsibility to the user
 - Users Form**
 - Active Users Report**

Oracle Application Security & Controls - Access

Function Security Menu report

Full Menu with Function Security
 Responsibility: Accounts Payable Manager
 Main Menu: AP_MANAGER_GUI

Level	Prompt	Sub Menu	Function	Description
1		AP_INVOICE_GATEWAY_GUI12		
2	Entry		Invoice Gateway	Enter Invoice Gateway Invoices
1	Invoices	AP_INVOICES_GUI12		Maintain Invoices
2	Entry	AP_INVOICES_ENTRY_GUI12		Invoices Entry
3	Invoice Batches	AP_APXINWKB_MENU	Invoice Batches	Maintain Invoice Batches
4			Invoice Actions	
4			Invoice Apply	
4			Prepayments	
4			Invoice Approve	
4			Invoice Cancel	
4		AP_APXINWKB_DISTSMENU	Invoice Distributions	
5			Invoice Distributions	
5			Prorate	
5			Invoice Distributions	
5			Reverse	
5			AP View Purchase Orders GUI	
5			JG Global Flexfield enabled flag	
5			Match to Receipts	Receipt Matching Form
5			Match to Purchase Order	Purchase Order Matching Form
5			Match to Invoice Receiving	Invoice Matching Form
5			Transaction Summary	
5			Charge Allocations	Charge Allocations Form
4			Invoice Fundscheck	
4			Invoice Holds	
4			Invoice Payments	
4			Invoice Match	
4			Invoice Payment Schedules	
4			Invoice Payments	



Oracle Application Security & Controls - Access

□ Users form

The screenshot shows the Oracle Users form with the following fields and sections:

- User Name:** [Text Field]
- Description:** [Text Field]
- Password:** [Text Field]
- Password Expiration:** Radio buttons for Days, Accesses, and None.
- Person:** [Text Field]
- Customer:** [Text Field]
- Supplier:** [Text Field]
- E-Mail:** [Text Field]
- Fax:** [Text Field]
- Effective Dates:** From [17/JAN/2001] To [Text Field]

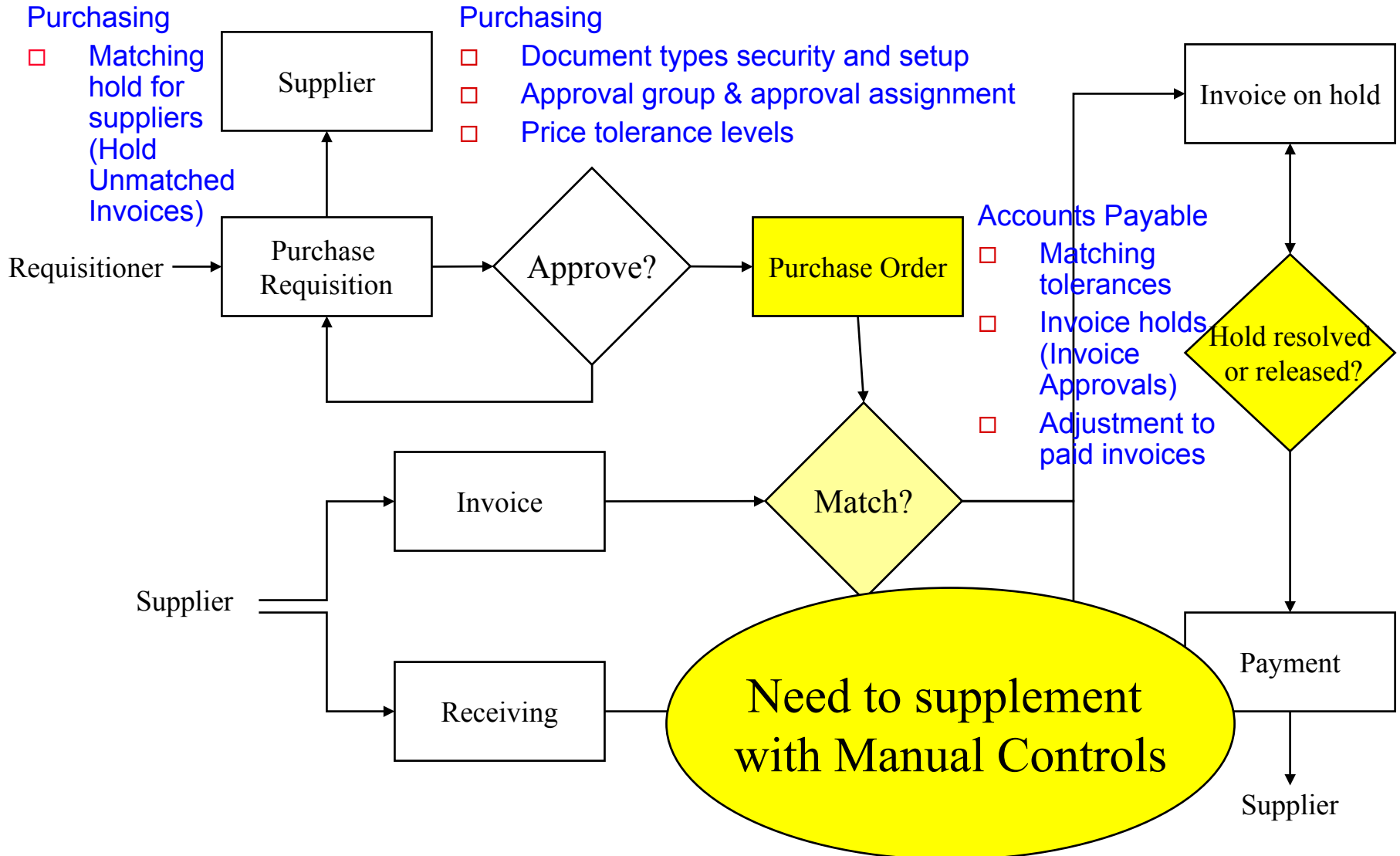
Below the form are two tabs: **Responsibilities** and **Securing Attributes**. The **Responsibilities** tab is active, showing a table with the following columns: Responsibility, Application, Security Group, From, and To.

Responsibility	Application	Security Group	From	To
[Text Field]	[Text Field]	[Text Field]	[Text Field]	[Text Field]
[Text Field]	[Text Field]	[Text Field]	[Text Field]	[Text Field]
[Text Field]	[Text Field]	[Text Field]	[Text Field]	[Text Field]
[Text Field]	[Text Field]	[Text Field]	[Text Field]	[Text Field]

Oracle Application Security & Controls - Access

- General access controls
 - Password related profile options (11i)
 - SIGNON_PASSWORD_FAILURE_LIMIT
 - SIGNON_PASSWORD_HARD_TO_GUESS
 - SIGNON_PASSWORD_LENGTH
 - SIGNON_PASSWORD_NO_REUSE

Oracle Application Security & Controls



Oracle Application Security & Controls

- **Resources**
 - **User guides**
 - **Technical reference manual**
 - **Help link via the application**
 - **Test environment**