
Enhanced Security Management, Separation of Duties and Audit Support for XA

Belinda Daub, Senior Consultant Technical Services

belinda.daub@cistech.net

704-814-0004

Agenda

Concepts, best practices, and tools to meet common XA security audit requirements:

- Separation of Duties
- Access Reviews
- **ES Version 5**
- R9 Security Considerations

Separation of Duties

Separation of Duties Concepts

- Separate duties so that no single person has control over the life of a transaction.
 - Initiate > Approve > Record > Reconcile > Audit
- To minimize risk, you must break the cycle
 - The greater the risk, the more it should be broken
- Common transaction cycles to audit
 - Purchase to Pay
 - Order to Cash
 - Personnel/Labor to Payroll
 - Administer system and maintain application data

Separation of Duties

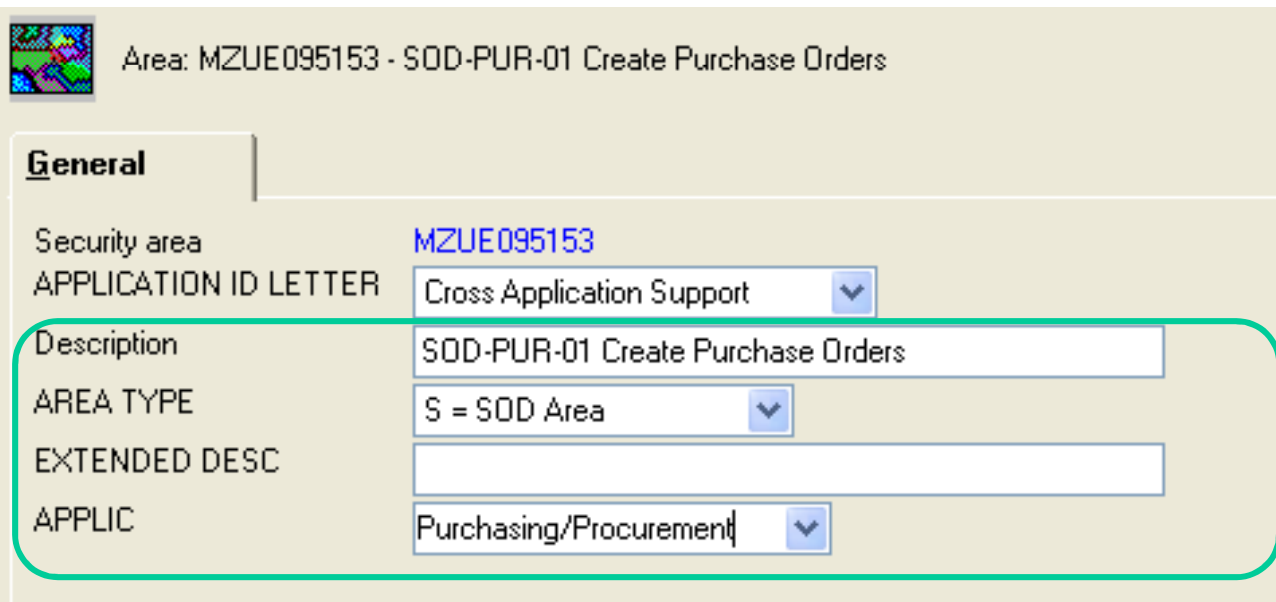
- What if you can't eliminate a conflict - Organization does not have sufficient personnel to separate responsibilities
 - Enforce controls to track activity and prove there is no abuse
- Your security was set up so that conflicts do not exist
 - How do you know that violations are not being created with ongoing security changes?
- How do you manage and report manual tasks involved in conflicts?
 - Monitor and report manually, OR
 - Track and report using CAS 'dummy' tasks

Separation of Duties

- Configure rules in Enhanced Security
 - Two conflicting functions
 - Configure rules by area or task or a combination of these
 - Any PO Create task can conflict with any AP Invoicing task
 - CAS, IFM and Custom Tasks
 - Manual tasks (bank deposits, handle cash...)
 - Define how violations should be addressed
 - Provide for mitigating or compensating controls if violations cannot be eliminated

ES SOD Management

- Create an SOD Area
 - SOD Areas represent a particular function
 - Maintain Purchase Orders, Create Vendors, Enter AP Invoices
 - New Fields to define and manage Functional Areas
 - Type
 - Extended Description
 - Actual Application involved
 - User Fields



The screenshot shows the SAP SOD Management configuration screen for a new SOD Area. The title bar reads "Area: MZUE095153 - SOD-PUR-01 Create Purchase Orders". The "General" tab is selected. The configuration fields are as follows:

Field	Value
Security area	MZUE095153
APPLICATION ID LETTER	Cross Application Support
Description	SOD-PUR-01 Create Purchase Orders
AREA TYPE	S = SOD Area
EXTENDED DESC	
APPLIC	Purchasing/Procurement

ES SOD Management

- Link Area to all tasks that are part of that function
 - Green screen
 - IFM
 - Power Link (create/copy/change/delete/maintain/mass maint)
 - Custom tasks

The screenshot displays the (EV) Environment Task application interface. The main window shows a table of tasks with columns for Task ID, Sub task ID, and Task description. A dialog box titled "(EV) Assign Task to an Area for Audit Reporting - Tas..." is open, showing configuration options for task AM6M2001.

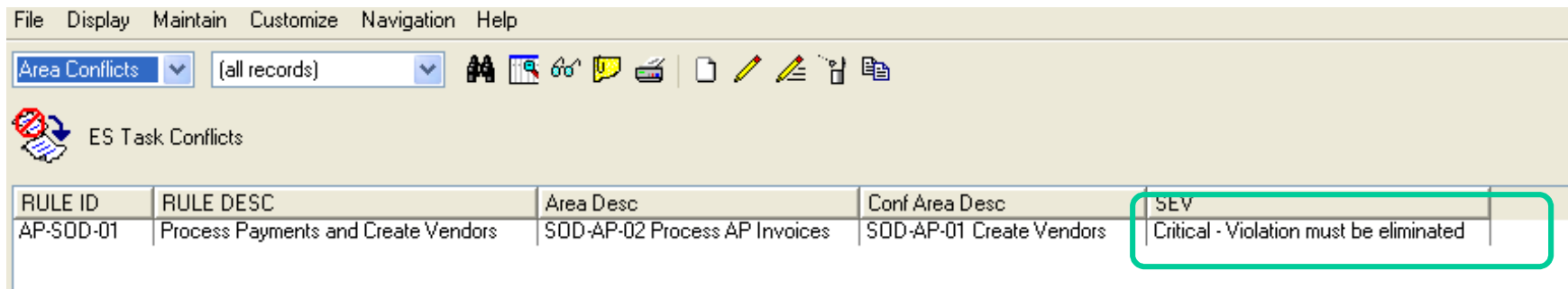
Task ID	Sub task ID	Task description
AM4GA	INS-TRNSTS	Commercial Invoice Send- Change Status
AM4GA	INS-TRNWS	Commercial Invoice Send- W/W Segments
AM6M2001		Enter/Edit Invoices and Credit Memos
AM6M2002		Enter/Edit Invoices & Cr Memos from Offline Fil
AM6M2002	DESC1	Enter/Edit Invoices & Cr Memos from Offline Fil
AM6M2003		Process Invoices and Credit Memos
AM6M2004		Post Invoices and Credit Memos
AM6M2005		EDI Invoices
AM6M2006		Print Invoice Reports
AM6M3007		Invoices and Credit Memos
AR5ADFR	ESIFM3	Work with Pseudo Invoice data
AR5BE1R	ESIFM3	Maintain Pseudo Invoice data
AR5YDFR	ESIFM3	Work with Pseudo Invoice
AR5ZE1R	ESIFM3	Maintain Pseudo Invoice

The dialog box configuration includes:

- Task: AM6M2001 - Enter/Edit Invoices and Credit Memos
- Template: Assign Audit Area
- AUDIT FLAG: Include Exclude
- Audit Area: MZUE105717
- TASK TYPE: Updates Data
- Preview before update
- Buttons: Update, Cancel, Help

ES SOD Management

- Define your SOD Conflict Rules
 - By Area or Task or combination



File Display Maintain Customize Navigation Help

Area Conflicts [all records]

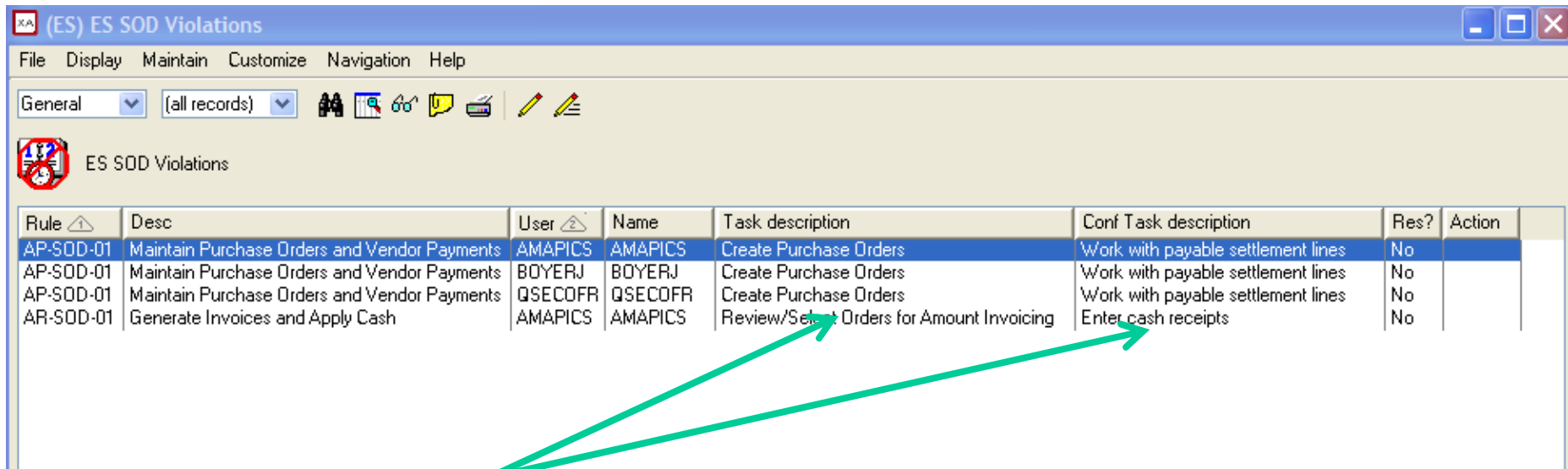
ES Task Conflicts

RULE ID	RULE DESC	Area Desc	Conf Area Desc	SEV
AP-SOD-01	Process Payments and Create Vendors	SOD-AP-02 Process AP Invoices	SOD-AP-01 Create Vendors	Critical - Violation must be eliminated

- Specify Severity
 - Critical – must be eliminated
 - Normal – requires mitigating control
- Attach documents
 - Separation of Duties Definition
 - Mitigating Control Details and Forms

ES SOD Management

- Periodically check to ensure you remain compliant



The screenshot shows a software window titled "(ES) ES SOD Violations". It features a menu bar (File, Display, Maintain, Customize, Navigation, Help), a toolbar with various icons, and a table of violations. The table has columns for Rule, Desc, User, Name, Task description, Conf Task description, Res?, and Action. Two red arrows point from the text below to the 'Task description' and 'Conf Task description' columns of the table.

Rule	Desc	User	Name	Task description	Conf Task description	Res?	Action
AP-SOD-01	Maintain Purchase Orders and Vendor Payments	AMAPICS	AMAPICS	Create Purchase Orders	Work with payable settlement lines	No	
AP-SOD-01	Maintain Purchase Orders and Vendor Payments	BOYERJ	BOYERJ	Create Purchase Orders	Work with payable settlement lines	No	
AP-SOD-01	Maintain Purchase Orders and Vendor Payments	QSECOFR	QSECOFR	Create Purchase Orders	Work with payable settlement lines	No	
AR-SOD-01	Generate Invoices and Apply Cash	AMAPICS	AMAPICS	Review/Select Orders for Amount Invoicing	Enter cash receipts	No	

- Individual tasks are shown for your convenience

Separation of Duties

- Managing and Resolving SOD Violations
 - Critical – Must be eliminated
 - Revoke authority to one or both tasks involved
 - Normal – Requires compensating control
 - Journaling
 - Detailed Transaction Review/Audit
 - Specific to the task involved
 - Thorough documentation
 - Track assignment/completion for security changes
 - Document change request or ticket information for reference

ES SOD Violation Resolution

KA (ES) Change ES SOD Violations - USER ID: AMAPICS - AMAPICS Rule: AP-SOD...

USER ID: AMAPICS - AMAPICS Rule: AP-SOD-01 - Maintain Purchase Orders and Vendor Payments

Template: (none)

Rule Description: Maintain Purchase Orders and Vendor Payments
Task: POR
Subtask: COPY
Conflicting Task: IFMTRAN
Conflicting Subtask: ESIFM1AP
Resolved Y/N: Yes No
Corrective Action: CTRL
Resolved by: DAUBB
Resolved Date: 11/01/2010
Resolved Time: 11:15:00 AM
Control Document: AP-SOD-01-C
Reference: 101102AMAPICS
Notes:

Auto advance
 Preview before update

Update Bypass Cancel Help

Action to take:

- Revoke authority to task
- Verify Compensating control
- Remove Conflict

Resolution tracking:

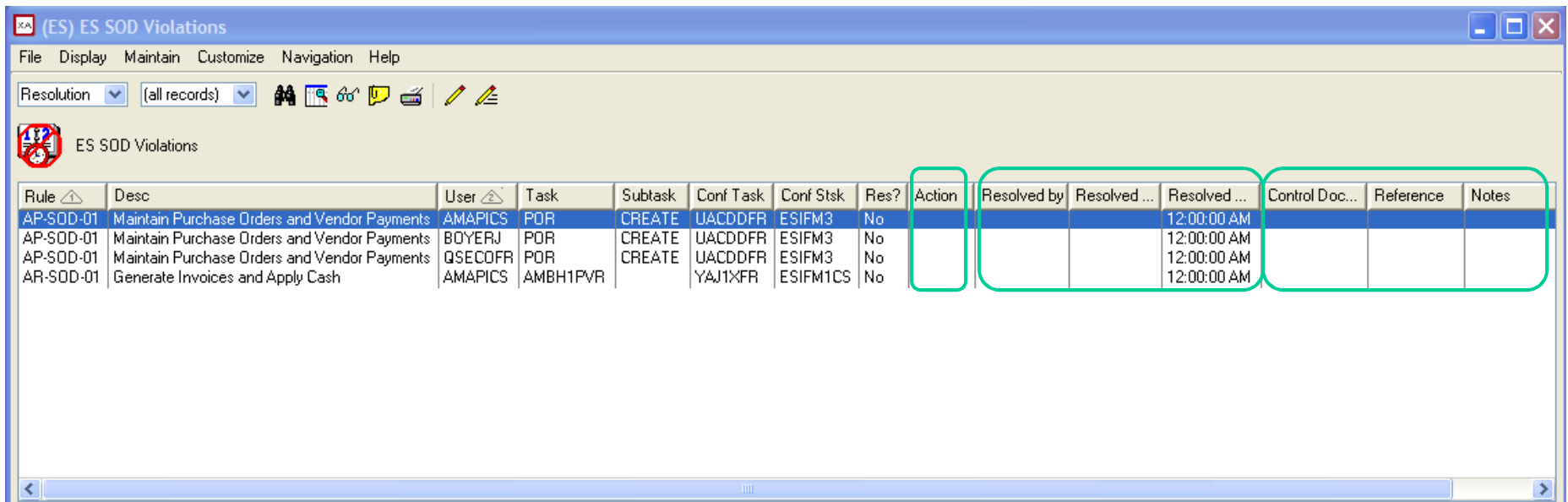
- Resolved by
- Date and Time

Reference Information:

- Control Document Number
- Reference for documentation specific to this violation
- Notes with information pertaining to the resolution or reason the conflict can be removed from the rules

ES SOD Management

- SOD Violations Review and Resolution



The screenshot shows the 'ES SOD Violations' application window. The window title is '(ES) ES SOD Violations'. The menu bar includes 'File', 'Display', 'Maintain', 'Customize', 'Navigation', and 'Help'. Below the menu bar, there is a toolbar with various icons. The main area displays a table with the following columns: Rule, Desc, User, Task, Subtask, Conf Task, Conf Stsk, Res?, Action, Resolved by, Resolved ..., Resolved ..., Control Doc..., Reference, and Notes. The table contains four rows of data, with the first row highlighted in blue. The 'Action' column is highlighted with a green box, and the 'Resolved by', 'Resolved ...', and 'Resolved ...' columns are grouped together with a green box.

Rule	Desc	User	Task	Subtask	Conf Task	Conf Stsk	Res?	Action	Resolved by	Resolved ...	Resolved ...	Control Doc...	Reference	Notes
AP-SOD-01	Maintain Purchase Orders and Vendor Payments	AMAPICS	POR	CREATE	UACDDFR	ESIFM3	No				12:00:00 AM			
AP-SOD-01	Maintain Purchase Orders and Vendor Payments	BOYERJ	POR	CREATE	UACDDFR	ESIFM3	No				12:00:00 AM			
AP-SOD-01	Maintain Purchase Orders and Vendor Payments	QSECOFR	POR	CREATE	UACDDFR	ESIFM3	No				12:00:00 AM			
AR-SOD-01	Generate Invoices and Apply Cash	AMAPICS	AMBHTPVR		YAJ1XFR	ESIFM1CS	No				12:00:00 AM			

- Manage resolutions within the application
- Track progress of resolution
- Assign security administrators to carry out resulting security changes
- Export or save review results when complete

Access Reviews

Access Review Concepts




- Insure users can perform only those tasks necessary for their assigned roles
- Insure data can be modified by only those who should have this authority
- Promote long-term integrity of security according to your defined policies
- Monitor access to high-risk tasks
- Confirm that all security changes have been made in accordance with internal controls

ES Access Review

- Two methods
 - Individual User Access
 - Role Access
- Security Review Coordinator
 - Schedule and facilitate review activities
 - Owner education and support
 - Generate review data and monitor progress
 - Coordinate and verify resolution activities

ES User Access Review

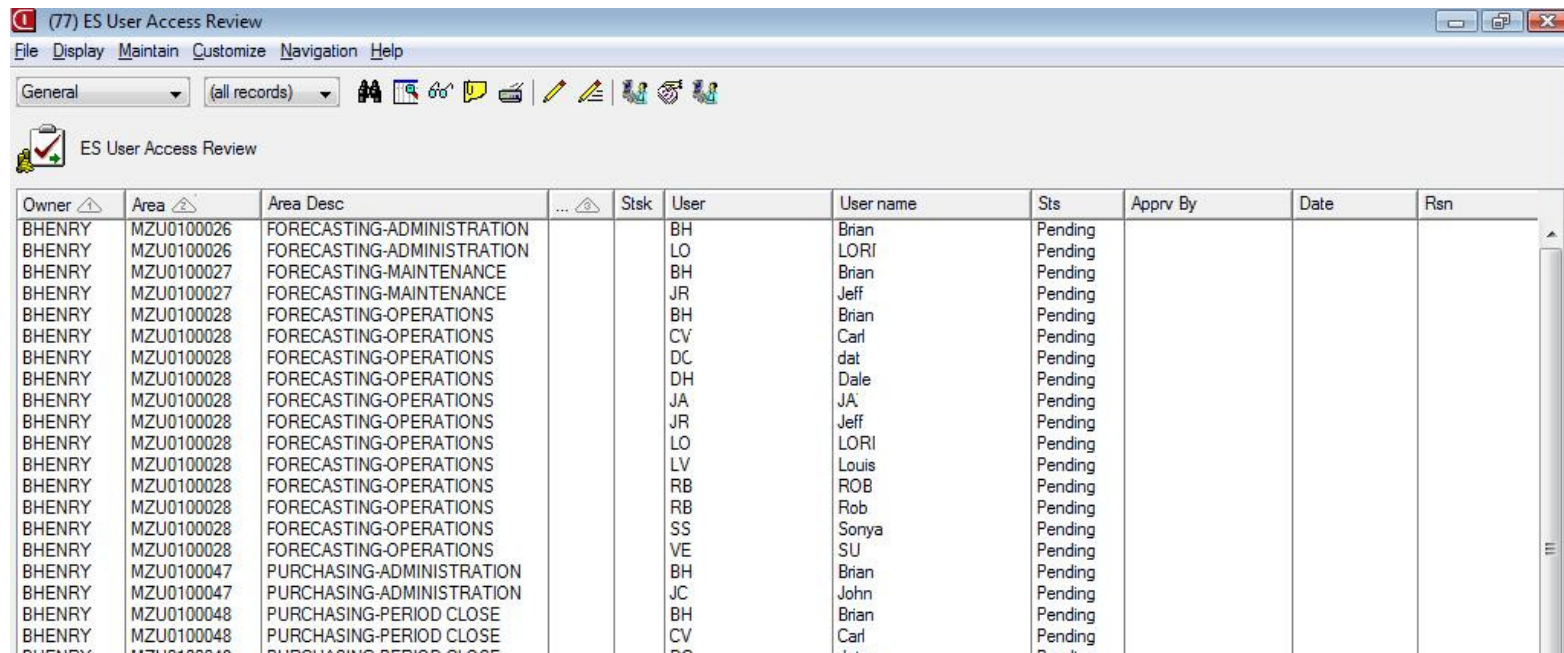
- Maintain Data Owners
 - This is done by functional area (group of tasks representing a particular set of data)
 - Use XA Areas or define your own for better organization

OWNER 	Name	AREA 	Desc	Co 	DEPT	AUDIT?	Task?	Unlck?	OVERRIDE DESC	OWNER APPROVER
DAUBB	DAUBB	AMZ SEC 01	CAS Security Mainte...	0		Yes	Yes	Yes	XA SECURITY MAINTENANCE	LUTHERD
LUTHERD	LUTHERD	AMZ SEC 04	CAS General Mainte...	0		Yes	No	No	CAS GENERAL SUPPORT TASKS	LUTHERD
DAUBB	DAUBB	AMZ SEC 27	Client Administration	0		Yes	No	No	XA CLIENT ADMINISTRATION AND MANAGEMENT	LUTHERD
LUTHERD	LUTHERD	MB0003	COM Invoicing	0		Yes	Yes	Yes	INVOICING CUSTOMERS	BENTONA

- Include or exclude an area in the review process
- Include Task details or just review at the area level
- Include/Exclude Unlocked Tasks in Area
- Owner Approver (owner cannot approve their own authority)

ES User Access Review

- Review Coordinator:
 - Generates User Access Data
 - Can view all owner records
 - Monitors progress (subset Pending status)
 - Coordinate Security Changes (subset Rejected status)
 - Request Archive of review data



The screenshot shows a software application window titled "(77) ES User Access Review". The window has a menu bar with "File", "Display", "Maintain", "Customize", "Navigation", and "Help". Below the menu bar is a toolbar with various icons. The main area of the window displays a table with the following columns: Owner, Area, Area Desc, Stsk, User, User name, Sts, Apprv By, Date, and Rsn. The table contains 20 rows of data, all with a "Pending" status.

Owner	Area	Area Desc	Stsk	User	User name	Sts	Apprv By	Date	Rsn
BHENRY	MZU0100026	FORECASTING-ADMINISTRATION		BH	Brian	Pending			
BHENRY	MZU0100026	FORECASTING-ADMINISTRATION		LO	LORI	Pending			
BHENRY	MZU0100027	FORECASTING-MAINTENANCE		BH	Brian	Pending			
BHENRY	MZU0100027	FORECASTING-MAINTENANCE		JR	Jeff	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		BH	Brian	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		CV	Carl	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		DC	dat	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		DH	Dale	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		JA	JA	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		JR	Jeff	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		LO	LORI	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		LV	Louis	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		RB	ROB	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		RB	Rob	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		SS	Sonya	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		VE	SU	Pending			
BHENRY	MZU0100047	PURCHASING-ADMINISTRATION		BH	Brian	Pending			
BHENRY	MZU0100047	PURCHASING-ADMINISTRATION		JC	John	Pending			
BHENRY	MZU0100048	PURCHASING-PERIOD CLOSE		BH	Brian	Pending			
BHENRY	MZU0100048	PURCHASING-PERIOD CLOSE		CV	Carl	Pending			
BHENRY	MZU0100048	PURCHASING-PERIOD CLOSE		DC	dat	Pending			

ES User Access Review

- Data Owners
 - Only have access to the records they must review
 - Approve or reject access including reason for rejection
 - Fields provided for assignment and tracking of rejected access
 - List grows shorter and is blank when they are done


Owner	Area	Area Desc	Stsk	User	User name	Sts	Apprv By	Date	Rsn
BHENRY	MZU0100026	FORECASTING-ADMINISTRATION		BH	Brian	Pending			
BHENRY	MZU0100026	FORECASTING-ADMINISTRATION		LO	LORI	Pending			
BHENRY	MZU0100027	FORECASTING-MAINTENANCE		BH	Brian	Pending			
BHENRY	MZU0100027	FORECASTING-MAINTENANCE		JR	Jeff	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		BH	Brian	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		CV	Carl	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		DC	dat	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		DH	Dale	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		JA	JA	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		JR	Jeff	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		LO	LORI	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		LV	Louis	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		RB	ROB	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		RB	Rob	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		SS	Sonya	Pending			
BHENRY	MZU0100028	FORECASTING-OPERATIONS		VE	SU	Pending			
BHENRY	MZU0100047	PURCHASING-ADMINISTRATION		BH	Brian	Pending			
BHENRY	MZU0100047	PURCHASING-ADMINISTRATION		JC	John	Pending			
BHENRY	MZU0100048	PURCHASING-PERIOD CLOSE		BH	Brian	Pending			
BHENRY	MZU0100048	PURCHASING-PERIOD CLOSE		CV	Carl	Pending			
BHENRY	MZU0100048	PURCHASING-PERIOD CLOSE		DC	dat	Pending			

ES Role Access Review

- Access Review for Role-Based Environments
 - Distribute responsibility for access reviews to
 - Role Owners - verify users assigned to the correct roles and what the roles can do in the application
 - Data Owners - verify role access to application data in their area of responsibility
 - More manageable and easier to understand
 - Great for installations with a lot of users in multiple locations

ES Role Access Review

- Review Coordinator will
 - Verify that Job Roles and Functional Areas (data) are assigned to correct individuals
 - Generate Role Review data
 - Monitor progress (subset Pending status)
 - Coordinate Role Changes (subset Rejected status)
 - Request Archive of review data



Review	Desc	Sts
ESDAAP	Area Task Review	Review not currently active
ESDARP	Data Access by Role	Review currently in process
ESROFP	Role-Task Access Review	Review not currently active
ESROUP	User-Role Assignment Review	Review not currently active

Lock/Unlock
Generate Data
Clear/Reset

ES Role Access Review

- Configure (or verify) Role Owners

The screenshot displays the 'ES Job Roles' interface. At the top, there are tabs for 'General', 'Role Summary', and 'Role Description'. The 'Role Description' tab is active, showing the text: 'IT SYSTEMS ADMINISTRATORS ARE RESPONSIBLE FOR SUPPORTING USERS, MONITORING SYSTEM OPERATIONS AND PERFORMING SECURITY ADMINISTRATION TASKS.' Below this is a table of roles. The 'IT' role is selected, and its details are shown in the 'Role Summary' tab. The 'Role Information' section shows the Job Role as 'IT', Role Description as 'IT Systems Administrator', and ROLE OWNER as 'DAUBB'. The 'Groups assigned to role' section lists 'GRPIT' (IT Support Group) and 'GRSECADM' (Security Administration). The 'Users with this role' section lists 'BENTONA' (Amanda) and 'MARY' (Mary). A green arrow points from the 'IT' role in the table to the 'Role Information' section, and another green arrow points from the 'Role Description' tab to the 'Role Summary' tab.

Role	Desc	ROLE OWNER	Owner name
IMCNT	Inventory Counts	LUTHERD	LUTHERD
TEST4	IT Developer	LUTHERD	LUTHERD
IT	IT Systems Administrator	DAUBB	DAUBB
IMCLK	Materials Clerk	LUTHERD	LUTHERD
IMRCV	Materials Receiving Clerk	LUTHERD	LUTHERD

Group	Group Name
GRPIT	IT Support Group
GRSECADM	Security Administration

USER ID	Name
BENTONA	Amanda
MARY	Mary

ES Role Access Review

- Role Owners review
 - users assigned to each role they own
 - Single update using tools in toolbar
 - Mass Change

...	Owner name	Role	Desc	User n...	Sts	REVIEW DATE
...	Belinda Daub	FNAP	AP Clerk	Debra ...	Rejected	01/21/2012
...	Belinda Daub	FNAP	AP Clerk	Shirley ...	Approved	01/21/2012
...	Belinda Daub	FNAP	AP Clerk	Erin Be...	Approved	01/21/2012
...	Belinda Daub	FNAP	AP Clerk	Anette ...	Approved	01/21/2012
...	Belinda Daub	FNAP	AP Clerk	Joye H...	Rejected	01/21/2012
...	Belinda Daub	FNAP	AP Clerk	Kristina ...	Approved	01/21/2012
...	Belinda Daub	FNAP	AP Clerk	Jennifer...	Approved	01/21/2012
...	Belinda Daub	FNAP	AP Clerk	Jessica ...	Approved	01/21/2012
...	Belinda Daub	FNAPA	AP Group Lead	Kellie G...	Approved	01/21/2012

ES Role Access Review

- Role Owners also review
 - Tasks or functional areas authorized to each role

The screenshot shows a software window titled "(MM) ES Data Access by Role Review". The window contains a menu bar (File, Display, Maintain, Customize, Navigation, Help), a toolbar with various icons, and a table of data. The table has columns for Owner, A/T, FUNCTION/TASK, Subt, DESCRIPTION, Role Desc, Status, REVIEW DATE, and REVIEWED BY. A green circle highlights the 'Status' column, which contains the text 'pending review' for all entries.

Owner ...	A/T	FUNCTION/TASK	Subt	DESCRIPTION	Role Desc	Status	REVIEW DATE	REVIEWED BY
qsecofr	Task		EXT0153TXN	Site Order Resolution	IT Admin	pending review		
qsecofr	Task		EXT0153TXN	Site Order Resolution	Master System User	pending review		
qsecofr	Task		EXT0153TXN	Site Order Resolution	Shop Floor Controller	Access Reviewed	07/26/2011	DAUBB
qsecofr	Task	ACCALLCMDS		Access to all commands (Application ...	IT Admin	pending review		
qsecofr	Task	ACCALLCMDS		Access to all commands (Application ...	Master System User	pending review		
qsecofr	Task	ACCMAPCMDS		Access to all Application commands	General Inquiry	pending review		
qsecofr	Task	ACCMAPCMDS		Access to all Application commands	Customer Admin	pending review		
qsecofr	Task	ACCMAPCMDS		Access to all Application commands	Loaner Scheduler	pending review		
qsecofr	Task	ACCMAPCMDS		Access to all Application commands	IT Admin	pending review		
qsecofr	Task	ACCMAPCMDS		Access to all Application commands	Master System User	pending review		
qsecofr	Task	ACCMAPCMDS		Access to all Application commands	Millstone Users	pending review		
qsecofr	Task	ACCMAPICS		Access to this environment	General Inquiry	pending review		
qsecofr	Task	ACCMAPICS		Access to this environment	Customer Admin	pending review		
qsecofr	Task	ACCMAPICS		Access to this environment	Loaner Scheduler	pending review		

ES Role Access Review

- Data Owners review
 - Role access to data
 - Same process as User Access Review, but by Role rather than User
 - Review at the task level or by functional area
 - Sorted by Task or Area but can sort other ways
 - List grows shorter as records are processed
 - Rejected access can be assigned to administrators and tracked

Data Owner ▲	Name	A/T	FUNCTION/TASK ▲	Subt ▲	DESCRIPTION	ROLE ID	Role Desc	Sts	REVIEW DATE	REVIEWED BY
DAUBB	DAUBB	Task	AMZ SEC	01	Security Maintenance	IT	IT			
DAUBB	DAUBB	Task	AMZM3801		Area and task authorizations	APCLK	AP Clerk			
DAUBB	DAUBB	Task	AMZM3801		Area and task authorizations	IT	IT			
DAUBB	DAUBB	Task	AMZM3801		Area and task authorizations	TEST	TEST Role			
DAUBB	DAUBB	Task	AMZM3802		User authorizations	IT	IT			
DAUBB	DAUBB	Task	AMZM3803		Data group and task authorizations	IT	IT			
DAUBB	DAUBB	Task	AMZM3805		Work With XA User Profiles	IT	IT			
LUTHERD	LUTH...	Area	AMZ SEC 04		Access to this environment	APCLK	AP Clerk			
LUTHERD	LUTH...	Area	AMZ SEC 04		Access to this environment	IT	IT			
LUTHERD	LUTH...	Area	AMZ SEC 04		Access to this environment	TEST	TEST Role			

ES Role Access Review

- Data Owners also review
 - Tasks that are defined as a functional area
 - Approve - all tasks represent the same data (Purchase Order, Inventory...)
 - Reject – area includes tasks that are not part of the area
 - These should be moved to another area OR
 - Data access for the functional area should be reviewed at the task level

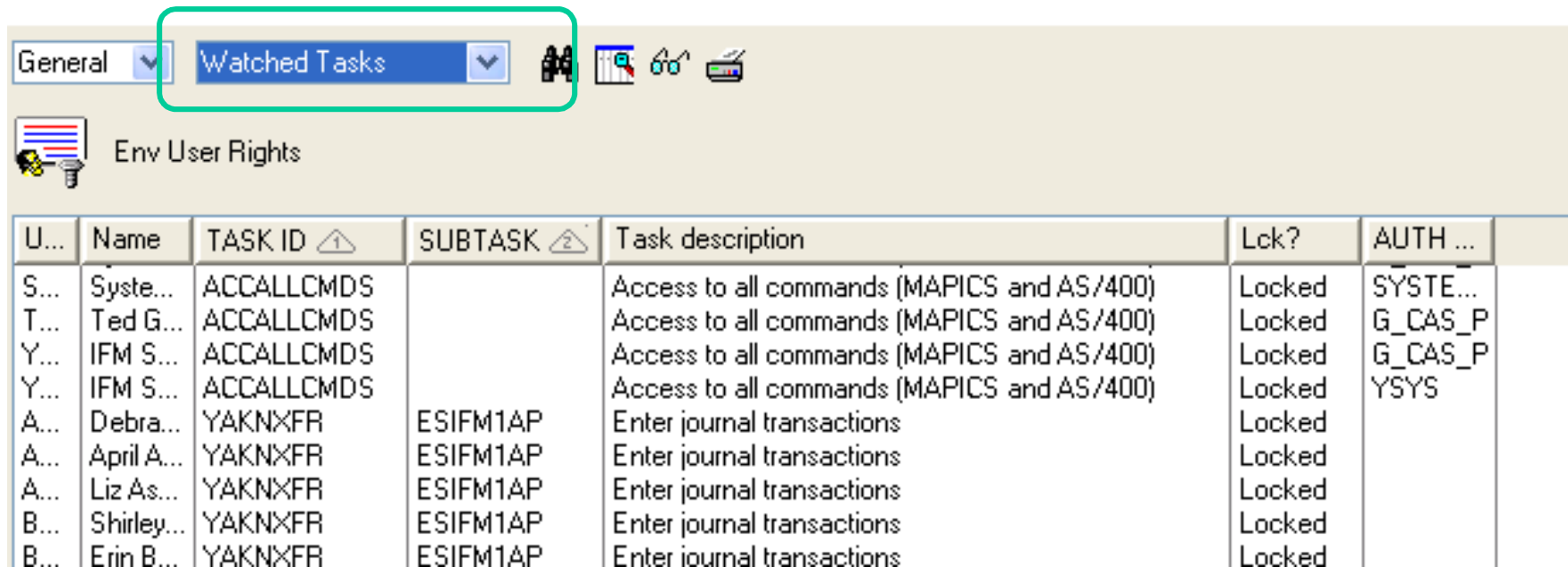
General (all records)

ES Area Task Review

Owner	Name	Area	Area Desc	Task	Subt	Task description	Sts	Rev by	REVIEW DATE
DAUBB	DAUBB	AMZ SEC 01	XA SECURITY MAINTENANCE	AMXWHSINQ		Inquiry Tasks	Approved	DAUBB	06/22/2012
DAUBB	DAUBB	AMZ SEC 01	XA SECURITY MAINTENANCE	AMXWHSUPD		Update Tasks	Approved	DAUBB	06/22/2012
DAUBB	DAUBB	AMZ SEC 01	XA SECURITY MAINTENANCE	AMZ SEC	01	Security Maintenance	pending review		
DAUBB	DAUBB	AMZ SEC 01	XA SECURITY MAINTENANCE	AMZM3801		Area and task authorizations	pending review		
DAUBB	DAUBB	AMZ SEC 01	XA SECURITY MAINTENANCE	AMZM3802		User authorizations	pending review		
DAUBB	DAUBB	AMZ SEC 01	XA SECURITY MAINTENANCE	AMZM3803		Data group and task authorizations	pending review		
DAUBB	DAUBB	AMZ SEC 01	XA SECURITY MAINTENANCE	AMZM3804		Generate reports	pending review		
DAUBB	DAUBB	AMZ SEC 01	XA SECURITY MAINTENANCE	AMZM3805		Work With XA User Profiles	pending review		
DAUBB	DAUBB	AMZ SEC 01	XA SECURITY MAINTENANCE	AMZM3806		Work with Client Data Connection User P...	pending review		
DAUBB	DAUBB	AMZ SEC 27	XA CLIENT ADMINISTRATION AN...	DEFINITION	ADMIN	Perform User Definition Administration	pending review		
DAUBB	DAUBB	AMZ SEC 27	XA CLIENT ADMINISTRATION AN...	DEFINITION	SECURITY	Assign Security Categories	pending review		
DAUBB	DAUBB	AMZ SEC 27	XA CLIENT ADMINISTRATION AN...	FIELDS	SECURITY	Assign Security Categories	pending review		
DAUBB	DAUBB	AMZ SEC 27	XA CLIENT ADMINISTRATION AN...	JAVASVRS	CONTROL	Control Java Servers	pending review		

ES Access Review

- Review Coordinator can also provide auditors information regarding access to high-risk tasks when requested
 - Watched Tasks
 - Subsets tailored to your needs
 - On demand
 - No need for custom code or IT resource involvement



U...	Name	TASK ID ▲	SUBTASK ▲	Task description	Lck?	AUTH ...
S...	Syste...	ACCALLCMDS		Access to all commands (MAPICS and AS/400)	Locked	SYSTE...
T...	Ted G...	ACCALLCMDS		Access to all commands (MAPICS and AS/400)	Locked	G_CAS_P
Y...	IFM S...	ACCALLCMDS		Access to all commands (MAPICS and AS/400)	Locked	G_CAS_P
Y...	IFM S...	ACCALLCMDS		Access to all commands (MAPICS and AS/400)	Locked	YSYS
A...	Debra...	YAKNXFR	ESIFM1AP	Enter journal transactions	Locked	
A...	April A...	YAKNXFR	ESIFM1AP	Enter journal transactions	Locked	
A...	Liz As...	YAKNXFR	ESIFM1AP	Enter journal transactions	Locked	
B...	Shirley...	YAKNXFR	ESIFM1AP	Enter journal transactions	Locked	
B...	Erin B...	YAKNXFR	ESIFM1AP	Enter journal transactions	Locked	

ES Access Review

- Review Private Authority
 - Exclude system and generic ids using subsets

Private Authorities							
Userid	Name	Task ID	Sub task ID	Task description	Lck?	Task type	Appli
AMAPICS	AMAPICS	AMZ SEC	01	Security Maintenance	Locked	GRP	CAS
AMAPICS	AMAPICS	DEFINITION	SECURITY	Assign Security Categories	Unlocked	SEC	CAS
AMAPICS	AMAPICS	FIELDS	SECURITY	Assign Security Categories	Unlocked	SEC	CAS
AMAPICS	AMAPICS	OBJECT	SECURITY	Assign Security for Business Objects	Unlocked	SEC	CAS
DAUBB	DAUBB	AMZ SEC	01	Security Maintenance	Locked	GRP	CAS
DAUBB	DAUBB	DEFINITION	SECURITY	Assign Security Categories	Unlocked	SEC	CAS
DAUBB	DAUBB	FIELDS	SECURITY	Assign Security Categories	Unlocked	SEC	CAS
DAUBB	DAUBB	OBJECT	SECURITY	Assign Security for Business Objects	Unlocked	SEC	CAS
LUTHERD	LUTHERD	AMZ SEC	01	Security Maintenance	Locked	GRP	CAS
LUTHERD	LUTHERD	DEFINITION	SECURITY	Assign Security Categories	Unlocked	SEC	CAS
LUTHERD	LUTHERD	FIELDS	SECURITY	Assign Security Categories	Unlocked	SEC	CAS
LUTHERD	LUTHERD	OBJECT	SECURITY	Assign Security for Business Objects	Unlocked	SEC	CAS

ES Access Review

- Review Unlocked Tasks Workbench
 - Who uses them
 - What XA Area controls the task

General | Unlocked

Environment Task

Task ID	Sub task ID	Task description	Applic	Lck?	Owner	Type
AMDM1001		Product Costing-Current	EPDM	Unlocked	MAPICS	MNT
AMDM1002		Product Costing-Standard	EPDM	Unlocked	MAPICS	MNT
AMDM1003		Product Costing-Both	EPDM	Unlocked	MAPICS	MNT
AMDM1004		Simulate Product Cost-Current	EPDM	Unlocked	MAPICS	MNT

(MR) Daily Task Activity - Task: AMDM1001 - Product ...

File | Display | Maintain | Customize | User | Navigation | Help

General | *(all records)

Task: AMDM1001 - Product Costing-Current

X...	Date	Time	AS/...	MAPICS MENU	OPTION	Lck?
KUMA...	111026	184,806	KU...	AMDM10	01	Unlocked
LABEL...	111008	110,059	LAB...	AMDM10	01	Unlocked

(MR) Areas containing task - Task: AMDM1001 - ...

File | Display | Maintain | Customize | Navigation | Help

General | *(all records)

Task: AMDM1001 - Product Costing-Current

Security...	Desc	Applic	Lck?	Owner
-------------	------	--------	------	-------

ES Access Review

- Review who has access to the environment

File Display Maintain Customize Navigation Help

General + (temporary) - Status

Environment Users

Name	Grp Jobs	U/G	Start Menu	OPID	Status	Last On
Susan...	0	User			*ENABLED	120105
Bruce...	0	User			*DISABLED	100708
James...	0	User	AMIM00		*ENABLED	120119
AGILE...	0	User			*ENABLED	120105
Daniel...	0	User	AMBM20		*ENABLED	
PR Mir...	0	User				
AMAP...	16	User				

- iSeries Profile disabled
- Enabled users who have not logged on recently

Special Authority Info Power Users

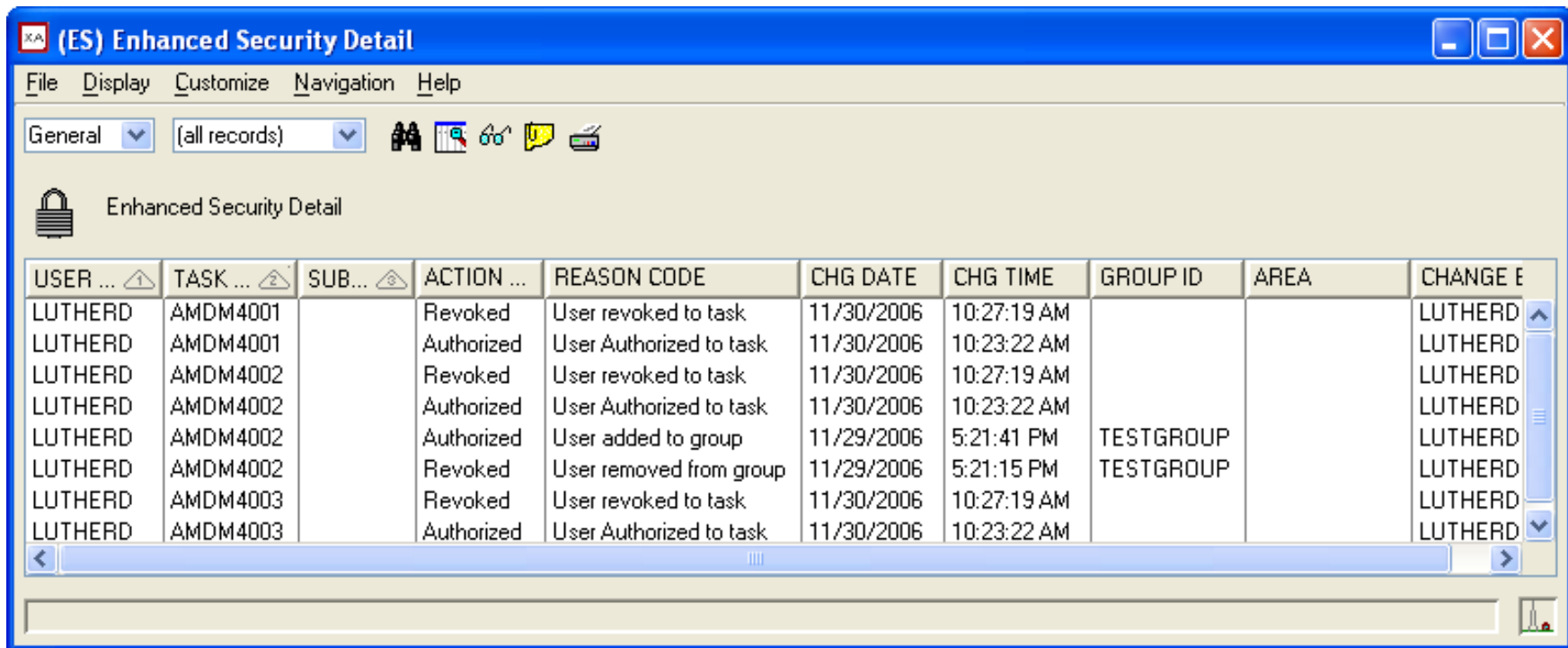
ES iSeries Profile Information

- Command line
- Special authorities

U...	Limit?	Special authorities
DEVI...	*YES	*JOBCTL
DEXT...	*YES	*JOBCTL
DIMIE...	*YES	*SPLCTL
DMIL...	*NO	*ALLOBJ *JOBCTL *SAVSYS *SERVICE *SPLCTL
DOS...	*YES	*JOBCTL
DPIG...	*NO	*JOBCTL

ES Access Review

- Review changes made to XA Security
 - Who made the change and when
 - Reconcile to security requests
 - Audit temporary access (granted and revoked in same day)



The screenshot shows a window titled "(ES) Enhanced Security Detail" with a menu bar (File, Display, Customize, Navigation, Help) and a toolbar. Below the toolbar is a lock icon and the text "Enhanced Security Detail". The main area contains a table with the following columns: USER, TASK, SUB, ACTION, REASON CODE, CHG DATE, CHG TIME, GROUP ID, AREA, and CHANGE E. The table lists several records for user LUTHERD, showing actions like "Revoked" and "Authorized" for tasks AMDM4001, AMDM4002, and AMDM4003. Two records show "Authorized" actions for "User added to group" with GROUP ID TESTGROUP.

USER ...	TASK ...	SUB...	ACTION ...	REASON CODE	CHG DATE	CHG TIME	GROUP ID	AREA	CHANGE E
LUTHERD	AMDM4001		Revoked	User revoked to task	11/30/2006	10:27:19 AM			LUTHERD
LUTHERD	AMDM4001		Authorized	User Authorized to task	11/30/2006	10:23:22 AM			LUTHERD
LUTHERD	AMDM4002		Revoked	User revoked to task	11/30/2006	10:27:19 AM			LUTHERD
LUTHERD	AMDM4002		Authorized	User Authorized to task	11/30/2006	10:23:22 AM			LUTHERD
LUTHERD	AMDM4002		Authorized	User added to group	11/29/2006	5:21:41 PM	TESTGROUP		LUTHERD
LUTHERD	AMDM4002		Revoked	User removed from group	11/29/2006	5:21:15 PM	TESTGROUP		LUTHERD
LUTHERD	AMDM4003		Revoked	User revoked to task	11/30/2006	10:27:19 AM			LUTHERD
LUTHERD	AMDM4003		Authorized	User Authorized to task	11/30/2006	10:23:22 AM			LUTHERD

ES Access Review

- Object Authorities – view and print
 - User rights to objects
 - XA objects not owned by AMAPICS
 - Public Authority

The screenshot shows the 'iSeries Object Authorities' window with a table listing various objects and their permissions. The table has columns for Object name, Library, Obj Type, User, AUTHORITY, and various permission flags (READ, ADD, DEL, UPD, EXEC, OPER, MGM, REF, ALTER, Group, PRI GRP, Owner, AUTLST SEC).

Object name	Library	Obj Type	User	AUTHORITY	READ	ADD	DEL	UPD	EXEC	OPER	MGM	REF	ALTER	Group	PRI GRP	Owner	AUTLST SEC
YAHQDFR	MXAMOD	*PGM	*PUBLIC	*EXCLUDE											*NONE	BOYERJ	*NONE
YAHQDFR	MXAMOD	*PGM	AMAPICS	*ALL	X	X	X	X	X	X	X	X	X		*NONE	BOYERJ	*NONE
YAHQDFR	MXAMOD	*PGM	BOYERJ	*ALL	X	X	X	X	X	X	X	X	X		*NONE	BOYERJ	*NONE
ARISS	MXAMOD	*QRYDFN	*PUBLIC	*CHANGE	X	X	X	X	X	X					*NONE	BOYERJ	*NONE
ARISS	MXAMOD	*QRYDFN	BOYERJ	*ALL	X	X	X	X	X		X	X	X		*NONE	BOYERJ	*NONE
CHECKS	MXAMOD	*QRYDFN	*PUBLIC	*CHANGE	X	X	X	X	X	X					*NONE	BOYERJ	*NONE
CHECKS	MXAMOD	*QRYDFN	BOYERJ	*ALL	X	X	X	X	X	X	X	X	X		*NONE	BOYERJ	*NONE
CSTDIF	MXAMOD	*QRYDFN	*PUBLIC	*CHANGE	X	X	X	X	X	X					*NONE	BOYERJ	*NONE
CSTDIF	MXAMOD	*QRYDFN	BOYERJ	*ALL	X	X	X	X	X	X	X	X	X		*NONE	BOYERJ	*NONE
ENTTOTBAL	MXAMOD	*QRYDFN	*PUBLIC	*CHANGE	X	X	X	X	X	X					*NONE	BOYERJ	*NONE
ENTTOTBAL	MXAMOD	*QRYDFN	BOYERJ	*ALL	X	X	X	X	X	X	X	X	X		*NONE	BOYERJ	*NONE
FINDERROR	MXAMOD	*QRYDFN	*PUBLIC	*CHANGE	X	X	X	X	X	X					*NONE	BOYERJ	*NONE
FINDERROR	MXAMOD	*QRYDFN	BOYERJ	*ALL	X	X	X	X	X	X	X	X	X		*NONE	BOYERJ	*NONE
FXFEB	MXAMOD	*QRYDFN	*PUBLIC	*CHANGE	X	X	X	X	X	X					*NONE	BOYERJ	*NONE
FXFEB	MXAMOD	*QRYDFN	BOYERJ	*ALL	X	X	X	X	X		X	X	X		*NONE	BOYERJ	*NONE
GLSUMEXT	MXAMOD	*FILE	*PUBLIC	*CHANGE	X	X	X	X	X	X					*NONE	BOYERJ	*NONE

Enhanced Security

Version 5

sneak peek

Enhanced Security **Version 5**

- Security Configuration Maintenance
 - Maintain Users and Groups
 - Lock/Unlock tasks
 - Freedom from hunting for tasks in application areas
 - Authorize Users and Groups to Tasks
 - Create Job Roles and Assign Users
 - Organize Tasks in to Areas for streamlining reviews and audits
 - SOD Violations Management
 - Data Owner Review of User Access
- Improvements in presentation and ease-of-use
 - Workspaces
 - Combo cards
 - User Exits (no more triggers)

Enhanced Security **Version 5**

- Work with Users
 - Add or delete users
 - Assign type of user (with subset capabilities)
 - Indicate whether to include in audits (omit system ids)
 - View system information for user (status/last on)

Userid	Name	U/G	Type	STS	Aud?	OPID	Last On	400 Status
AMAPICS	AMAPICS	User	General User	Active	Include		101109	*ENABLED
ANDY	ANDY	User	General User	Active	Include			
BENET	BENET	User	General User	Active	Include			
BENTONA	Amanda	User	General User	Active	Include	AB	100621	*ENABLED
BOYERJ	Jim B	User	General User	Active	Include	JB	120217	*ENABLED
CURLEEJ	Judi Curlee	User	General User	Active	Include	JC	120314	*ENABLED
DAUBB	DAUBB	User	General User	Active	Include		100621	*ENABLED
HOYESM	Mike Hoyes	User	General User	Active	Include		120223	*ENABLED
LEXEL	LEXEL	User	System or Application User	Active	Exclude			
LUTHERD	LUTHERD	User	General User	Active	Include		120314	*ENABLED
MARY	Mary	User	General User	Active	Include	MPC		

Enhanced Security **Version 5**

User Details

- User information
- Assigned Roles
- Assigned Groups

The screenshot shows a web-based application window titled "User Info" with a menu bar (File, Display, Maintain, Customize, Navigation, Help) and a toolbar. The user is identified as "Userid: DAUBB - DAUBB". The "User Summary" section displays the following details:

Userid	DAUBB	Initial Program	*NONE
User name	DAUBB	Initial menu	MAIN
TYPE	General User	Limit device sessions	*SYSVAL
STATUS	Active	Password change date: YYMMDD	100621
Audit?	Include	Previous sign-on date: YYMMDD	100621
User group code	User	Sign-on attempts not valid	0
		Status	*ENABLED

Below the summary are two tables:

Roles assigned to User

JOB ROLE	Desc
TEST4	IT Developer

Groups user is in

User group ID	Group name
GRPIT	IT Support Group
GRSECADM	Security Administration

At the bottom of the window are "Continue" and "Help" buttons.

Enhanced Security **Version 5**

Add or Delete Groups

The screenshot displays the 'Work with Groups' application interface. At the top, there is a menu bar with 'File', 'Display', 'Maintain', 'Customize', 'Navigation', and 'Help'. Below the menu bar, there are two dropdown menus: 'Group Info' and '* (all records)'. A toolbar with various icons is located to the right of the dropdowns. The main area is titled 'Work with Groups' and contains a table of group information.

Userid	Name	U/G	STS
ACCOUNTING	Accounting Department	Group	Active
GRCBASE	Customer Service Base	Group	Active
GRPIT	IT Support Group	Group	Active
GRSECADM	Security Administration	Group	Active
IMBASIC	Inventory - Basic Access	Group	Active

Below the table, there are two panels: 'Group Summary' and 'Group Info'. The 'Group Info' panel shows details for the selected group (GRSECADM - Security Administration):

- Userid: GRSECADM
- User name: Security Administration
- User group code: Group

The 'Group Authority to Tasks' panel shows a table of tasks:

Task ID	Sub task ID	Task description
AMZ SEC	01	Security Maintenance
AMZM3801		Area and task authorizations
AMZM3802		User authorizations
AMZM3803		Data group and task authorizations

The 'Group Members' panel shows a table of users:

User ID	User name
BENTONA	Amanda
DAUBB	DAUBB
LUTHERD	LUTHERD
MARY	Mary

At the bottom of the interface, there are two buttons: 'Continue' and 'Help'.

Group Details

- Group information
- Authorized Tasks
- Members

Enhanced Security

Simplified User Role Maintenance

- PowerLink workbench
- Roles match form
- Add or remove user roles

Add a user to a role

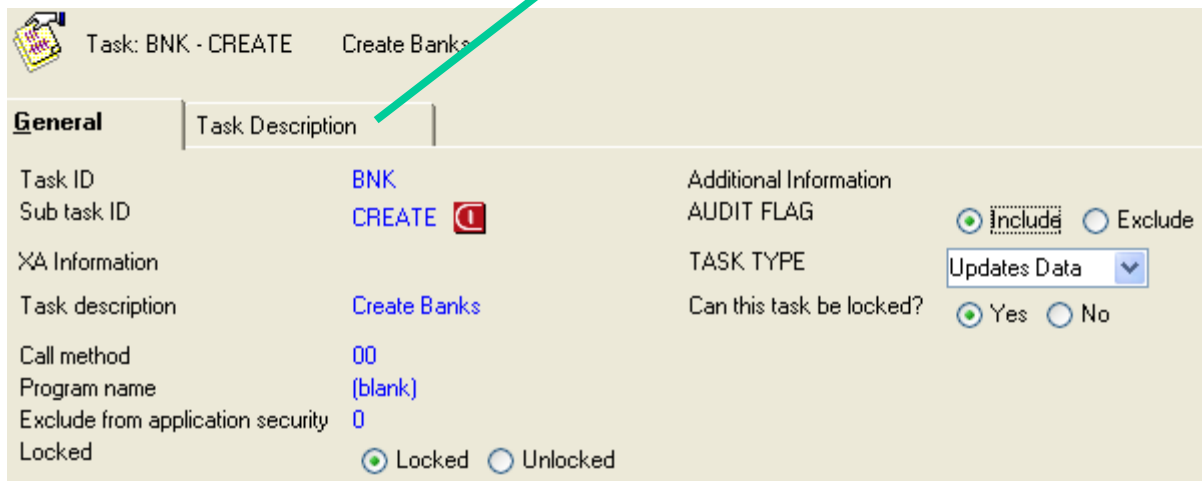
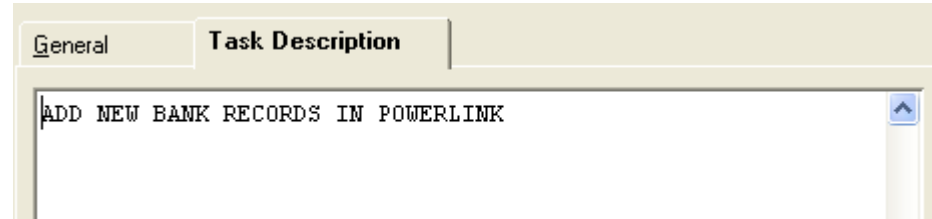
The screenshot shows two windows from the PowerLink workbench. The left window, titled 'Environment Users', displays a list of users. The right window, titled 'Userid: ARNOLDBY - Bradley Arnold', displays a table of job roles.

Job Role	Desc	Status
COGEN	General Inquiry	Active
COREQ	Requisition	Active
MPENG	MFG-PRC Engineer	Active



Enhanced Security **Version 5**

Task Maintenance

- Lock/Unlock
- Authorize users to tasks
- Assign task to Area



A screenshot of the 'Task Maintenance' interface showing the 'General' tab for a task named 'BNK - CREATE'. The task description is 'Create Banks'. The interface includes various configuration options:

Task ID	BNK	Additional Information	
Sub task ID	CREATE 	AUDIT FLAG	<input checked="" type="radio"/> Include <input type="radio"/> Exclude
XA Information		TASK TYPE	Updates Data 
Task description	Create Banks	Can this task be locked?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Call method	00		
Program name	(blank)		
Exclude from application security	0		
Locked	<input checked="" type="radio"/> Locked <input type="radio"/> Unlocked		

Additional fields

- Audit options
- Type of Task
- Flag tasks to be left unlocked
- Text Description

R9 Security Considerations

R9 Security Considerations

- At R7.8 Infor began moving IFM tasks to PowerLink
 - Secured using CAS Security
 - You must lock and authorize appropriate personnel
 - Corresponding green-screen tasks are still secured by IFM
- If you configure security in your test environment during R9 implementation, you need to plan for replicating this after each test migration and at go-live
- Your auditors will want supporting documentation for any security changes made

R9 Security Considerations

- IDF Level 1 considerations
 - IFM
 - Access to tasks is still controlled by IFM Security
 - Lock these if you want to turn off some or all of these tasks (roll them out as users are trained...)
 - Other Applications
 - IDF L1 tasks control access to the application functions
 - Lock these and authorize users as appropriate

R9 Security Considerations

- R9 Migration Assistance
 - CISTECH Migration Pack includes a free assessment
 - Analysis of your security configuration and recommendations
 - Extract list of new R9 tasks you will need to secure
 - Recommendations for managing your R9 Security Migration tasks
 - CISTECH R9 Security Migration Assistance includes tools and services during your migration to the new release
 - Assistance with planning your R9 Security migration
 - Customize template map to your applications
 - Programmatically set authority to new R9 tasks the same as equivalent tasks in IFM or green screen
 - Fine-tune during training/testing
 - Run after each XA re-migration and after live migration

Enhanced Security at XAR9

- For existing ES Installations
 - R9 compatibility requires upgrade to ES V5.0
 - General availability in mid-July 2012
 - Plan ahead
 - Contact productsupport@cistech.net for requesting R9 migration information

Thank you!

Questions?