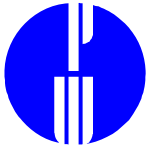
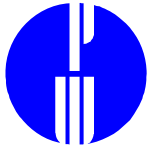
THIS PUBLICATION CONSISTS OF SIX SECTIONS
IN SEQUENTIAL ORDER

1. Introduction



Relational Data
Relational Database Architecture
Operating System Security vs Database Security



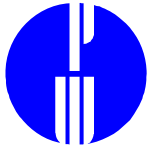
A DATABASE:

employee file

NAME	SSN	ADDR	PHONE	DT HIRE
Jim Jones	123-214-4572	xxxx	555-1212	3/20/90
Eve Smith	893-234-4567	xxxxx	555-2345	4/12/76
Mike Coll	123-784-4622	xxxxx	555-9999	12/4/89
Linda Till	993-234-4067	xxxxx	555-2343	2/3/94
.....				

payroll file

SSN	LEVEL	SALARY	PERIOD
251-646-7533	Staff	$25,000	weekly
576-124-6656	Super	$50,000	bi-monthly
123-214-4572	Staff	$25,000	monthly
893-234-4567	DH	$75,000	bi-monthly
.....			



A RELATIONAL DATABASE:

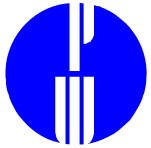
personnel database file

employee table

name
ssn
address
phone
date_hired

payroll table

ssn
level
salaru
period
qtd tax
ytd tax



GETTING DATA FROM A DATABASE:

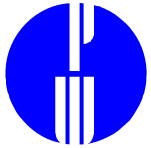
employee file

NAME	SSN	ADDR	PHONE	DT HIRE
Jim Jones	123-214-4572	xxxx	555-1212	3/20/90
Eve Smith	893-234-4567	xxxxx	555-2345	4/12/76
Mike Coll	123-784-4622	xxxxx	555-9999	12/4/89
Linda Till	993-234-4067	xxxxx	555-2343	2/3/94
.....				

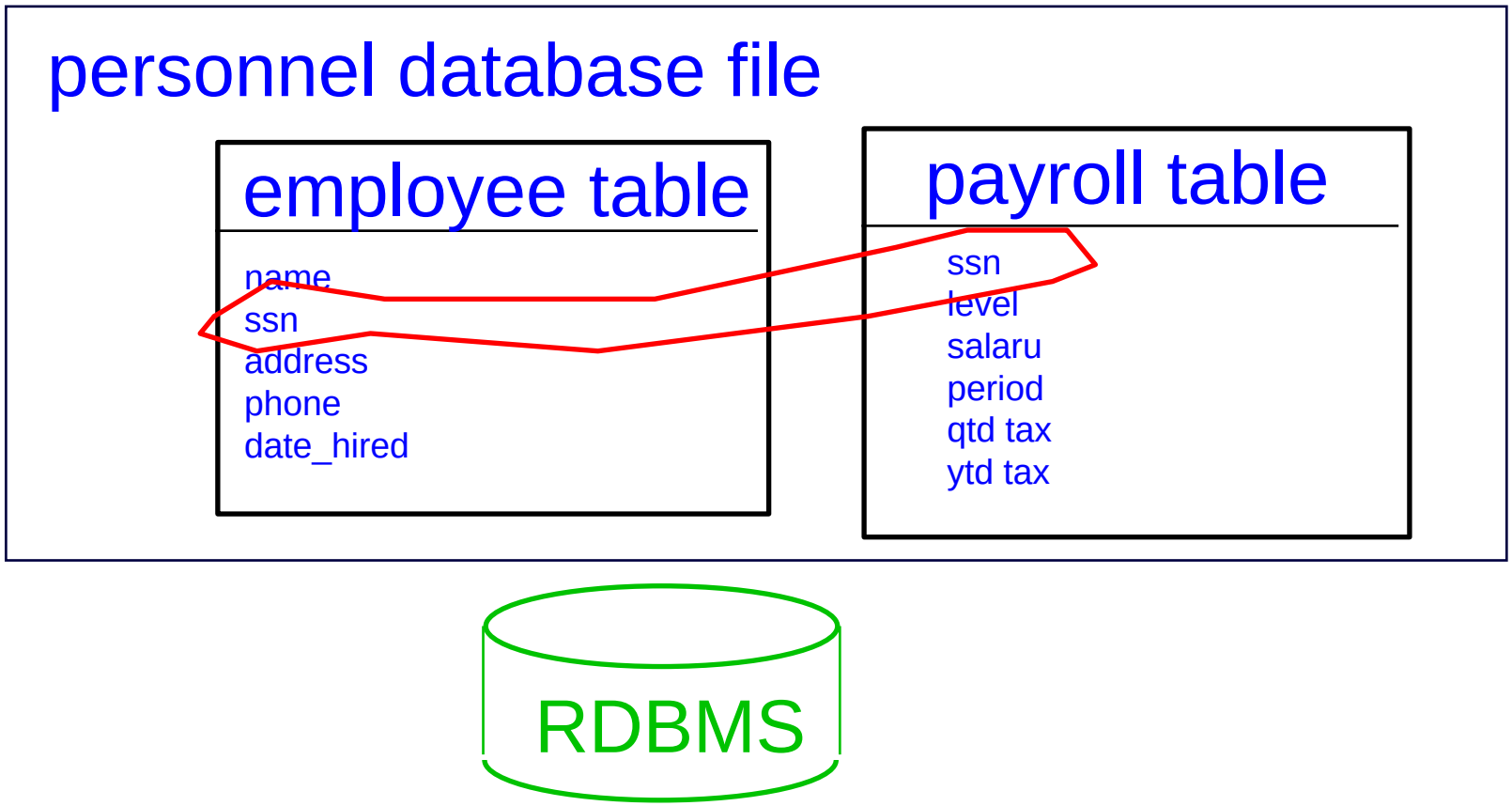
payroll file

SSN	LEVEL	SALARY	PERIOD
251-646-7533	Staff	$25,000	weekly
576-124-6656	Super	$50,000	bi-monthly
123-214-4572	Staff	$25,000	monthly
993-234-4567	DH	$75,000	bi-monthly
....			

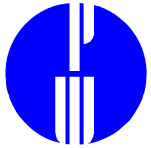
TWO COMMANDS



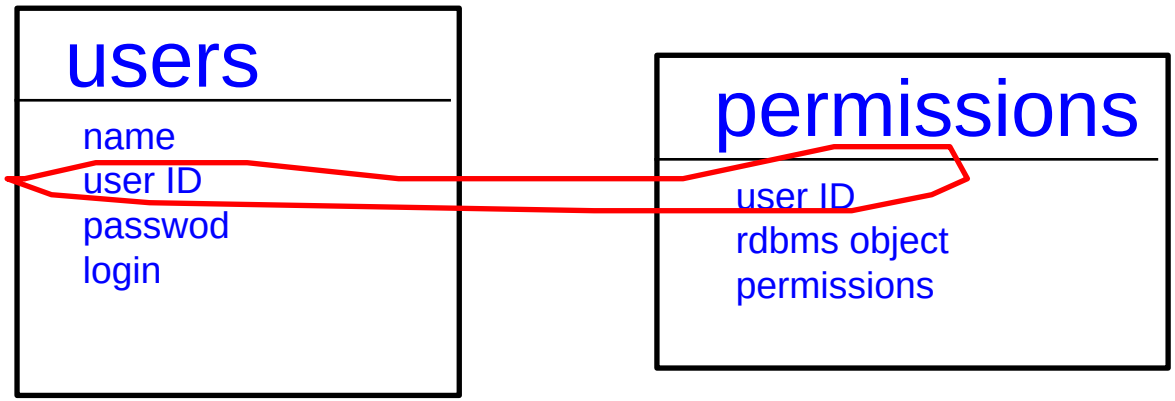
GETTING DATA FROM A RELATIONAL DATABASE:



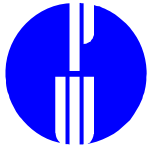
ONE COMMAND



INFORMATION ON ACCESS TO A RELATIONAL DATABASE:

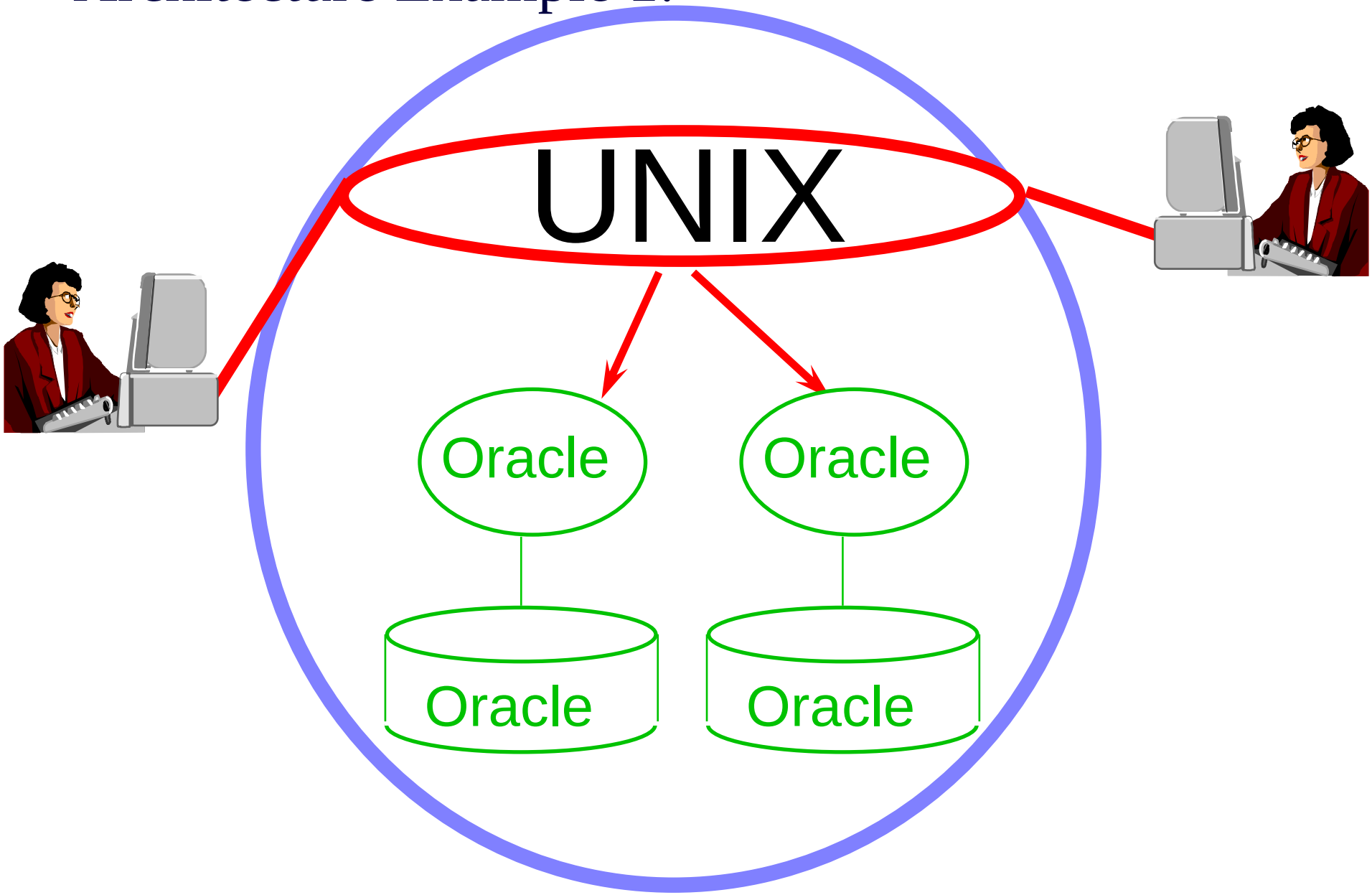


IS STORED JUST LIKE THE RELATIONAL DATA

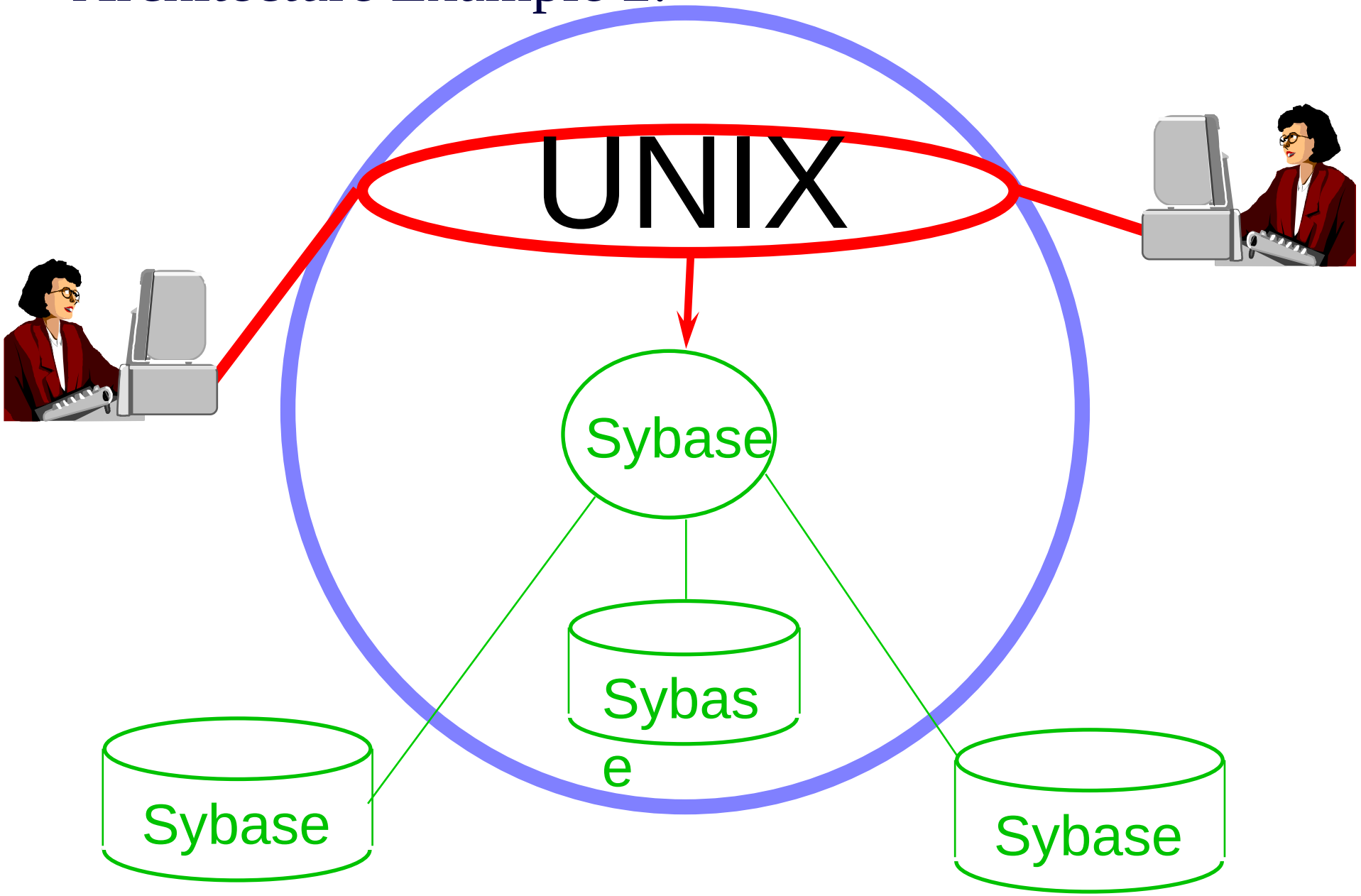


Question:
Do we need to care about controlling a relational database if we know the computer's operating system is well controlled?

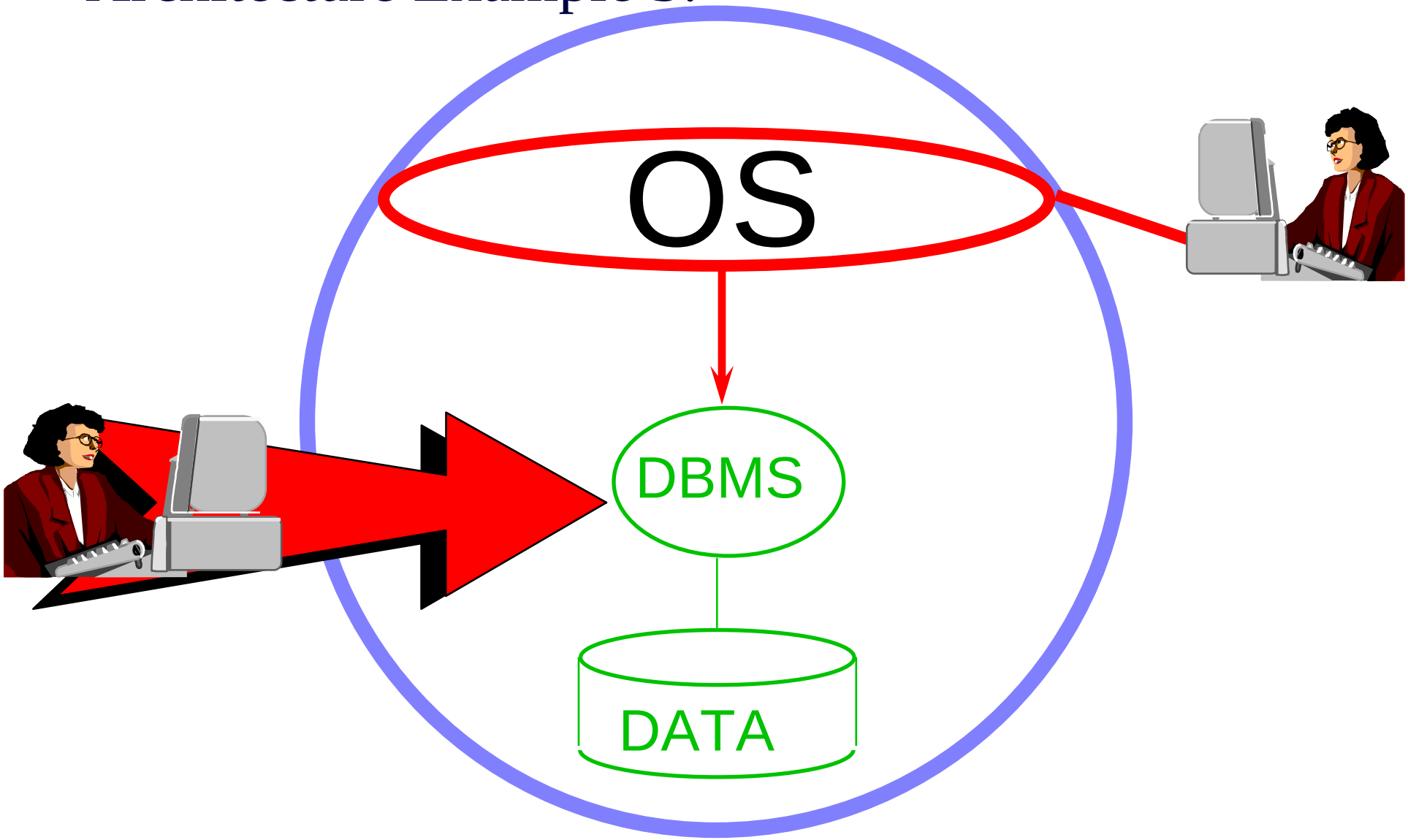
Architecture Example 1:

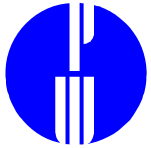


Architecture Example 2:



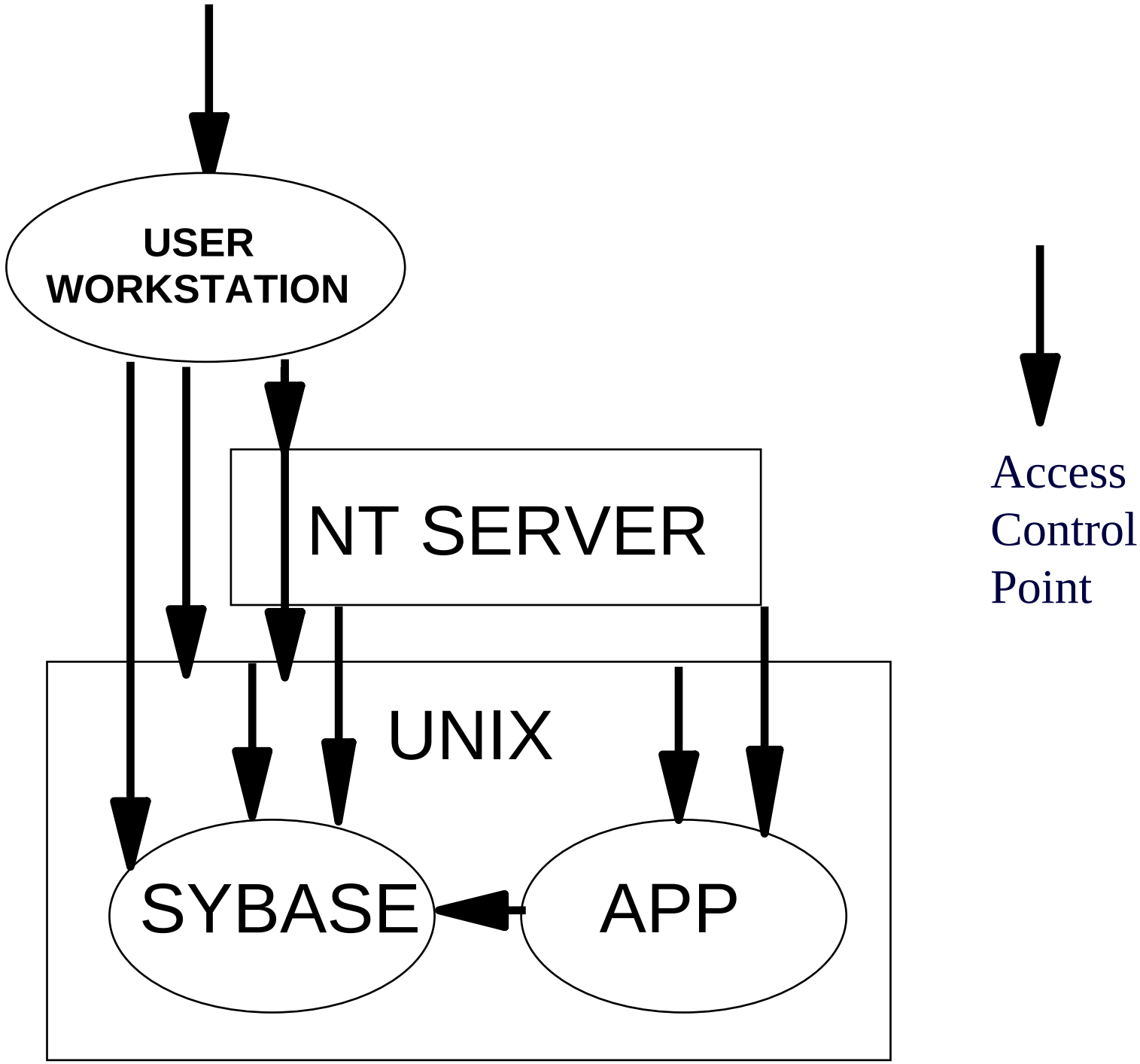
Architecture Example 3:





Question:
Do we need to care about controlling a relational database if we know the operating system is well controlled?

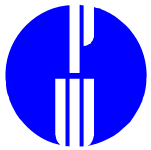
Answer:
Yes, the most popular relational database architectures allow users to access the relational database management system without requiring operating system authentication.


USER
WORKSTATION
NT SERVER
UNIX
SYBASE
APP
Access
Control
Point

Operating System Security vs Database Security

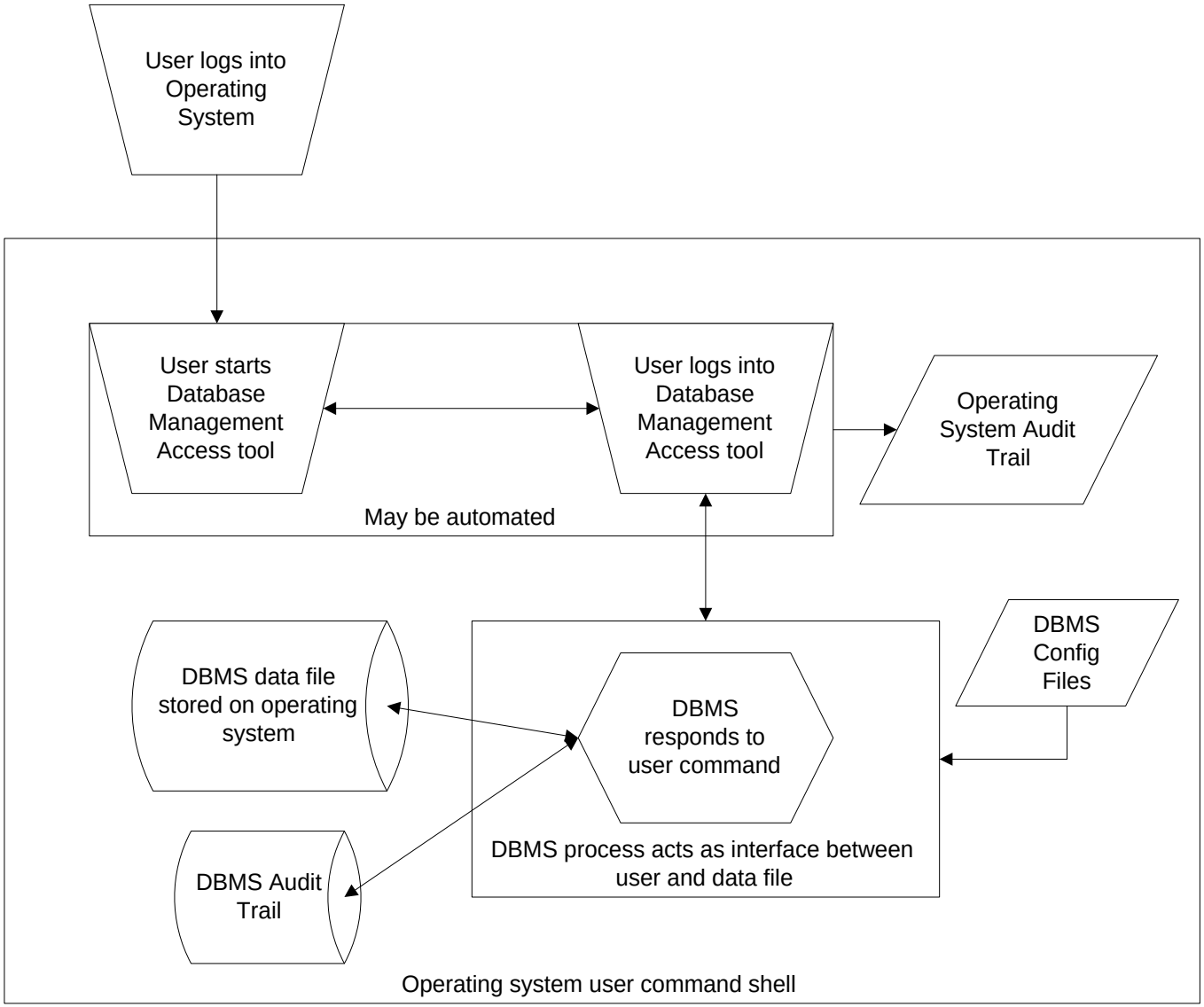
- OS
  - Rights to execute and/or manipulate DBMS program files
  - Rights to copy, rename, or corrupt DBMS data files stored as OS files
- DBMS
  - Rights to tables within DBMS data files
  - Rights to create and execute procedures that manipluate table structure and data

OS Security for DBMS

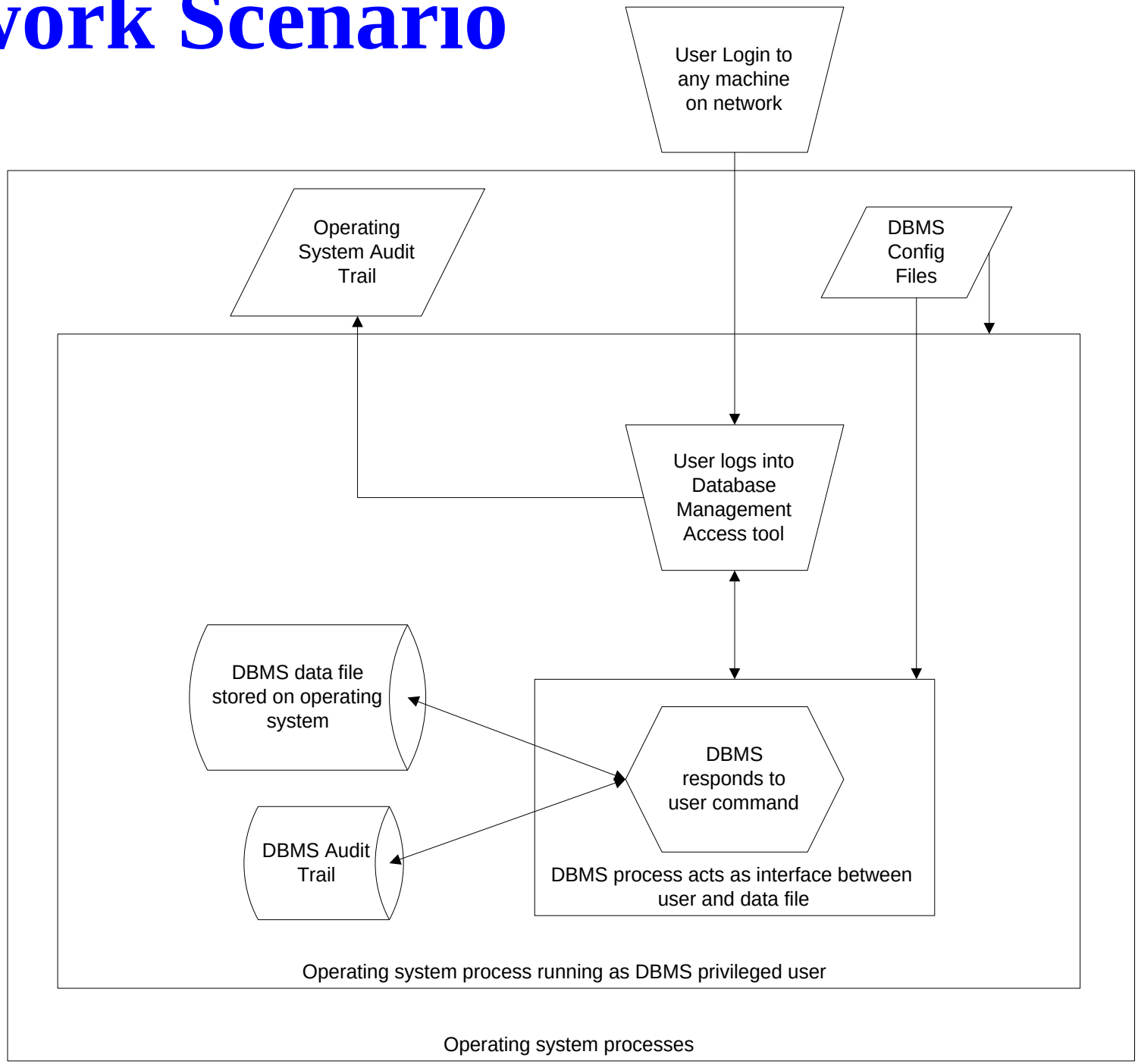


OS security treats the DBMS program and data files *just like any other operating system files*.
For example, it may be configured to restrict access to the Database Management System to a certain set of operating system users.

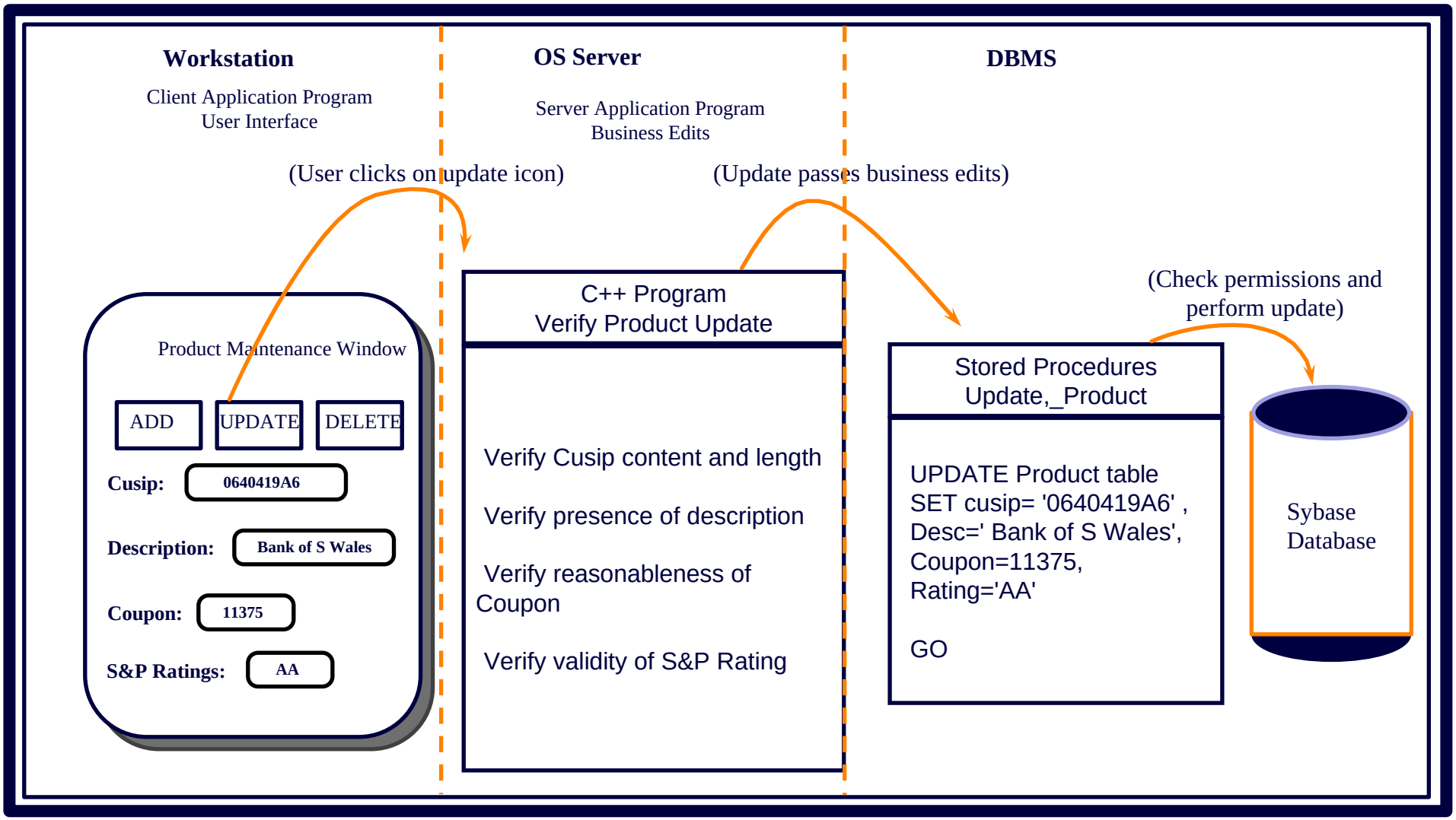
OS Scenario


User logs into Operating System
User starts Database Management Access tool
User logs into Database Management Access tool
Operating System Audit Trail
May be automated
DBMS data file stored on operating system
DBMS responds to user command
DBMS Config Files
DBMS Audit Trail
DBMS process acts as interface between user and data file
Operating system user command shell

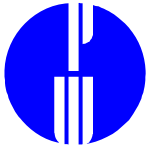
Network Scenario



Application Scenario



2. Organizational Environment

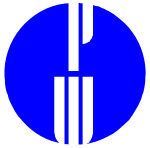


Roles and Responsibilities
Segregation of Duties
Caveats for Outsourcing

Database Management System
Audit and Control Responsibilties

- PREVENTION
- DETECTION
- RECOVERY

Prevention

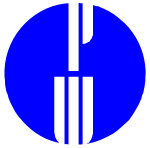


- Configure database environment
- Add and delete database users

Detection

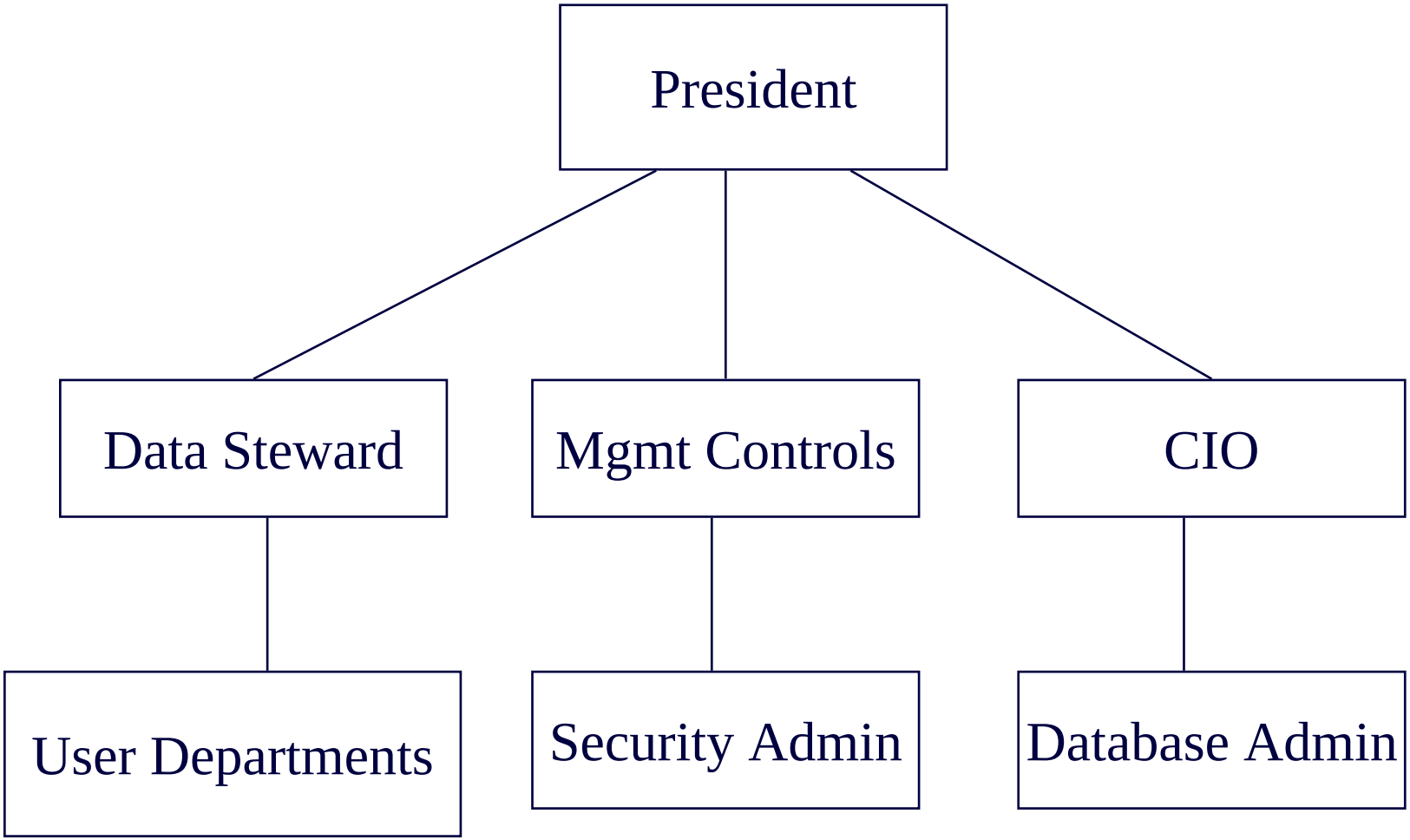
- Audit data access
- Audit failed access attempts
- Audit DBMS configuration
- Maintain integrity of audit trail
- Monitor changes to database structure

Recovery



- Develop “back-out scenarios” for database management system and/or database schema changes
- Plan and automate database backup and recovery mechanisms

Sample Org Chart



Database Administrator (DBA) Sample Job Description

- Create and maintain hardware and software requirements for data storage and retrieval
- Automate DBMS startup and shutdown
- Specify and maintain DBMS configuration
- Maintain inventory of DBMS information resources
- Develop and maintain database backup and recovery procedures
- Create and implement tools that automate database monitoring
- Analyze database management system performance
- Assist help desk, operating system, and application support personnel in resolving system problems

Security Administrator (SA) Sample Job Description

- Create and maintain user accounts on production systems
- Specify audit trail configuration
- Monitor audit trails
- Track and provide reporting related to policy exceptions
- Review changes to production environment for possible security impact
- Provide security awareness training to database, network, and operating system administrators

Data Steward (DS)
Sample Job Description

In addition to business process related functions, manage the generation and storage of data created by the department and/or used by the department for business purposes.

- Ensure data completeness
- Ensure data accuracy
- Periodically audit data integrity

Role of the Database Admin

PREVENTION:

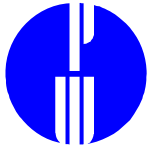
- Configure database environment
- Add and delete database users

DETECTION:

- Audit data access
- Audit failed access attempts
- Audit DBMS configuration
- Maintain integrity of audit trail
- Monitor changes to database structure

RECOVERY:

- Develop “back-out scenarios” for database management system and/or database schema changes
- Plan and automate database backup and recovery mechanisms



Role of the Security Admin

PREVENTION:

- Configure database environment
- Add and delete database users

DETECTION:

- Audit data access
- Audit failed access attempts
- Audit DBMS configuration
- Maintain integrity of audit trail
- Monitor changes to database structure

RECOVERY:

- Develop “back-out scenarios” for database management system and/or database schema changes
- Plan and automate database backup and recovery mechanisms

Role of the Data Steward

PREVENTION:

- Configure database environment
- Add and delete database users

DETECTION:

- Audit data access
- Audit failed access attempts
- Audit DBMS configuration
- Maintain integrity of audit trail
- Monitor changes to database structure

RECOVERY:

- Develop “back-out scenarios” for database management system and/or database schema changes
- Plan and automate database backup and recovery mechanisms

Segregation of Prevention Duties

PREVENTION:

- DBA: Configure database environment
  - Add SA as a user who can add & delete end-users
  - Create user groups and associated data access according to application requirements
  - Configure audit trails to audit DBA actions
  - Configure audit trails to monitor changes in configuration
  - Work with OS admin to ensure only security admin may alter audit trails
- SA: Add and delete database users
  - Ensure that each user least amount of privileges required for job function
  - Maintain list of authorized users

Segregation of Detection Duties

DETECTION:

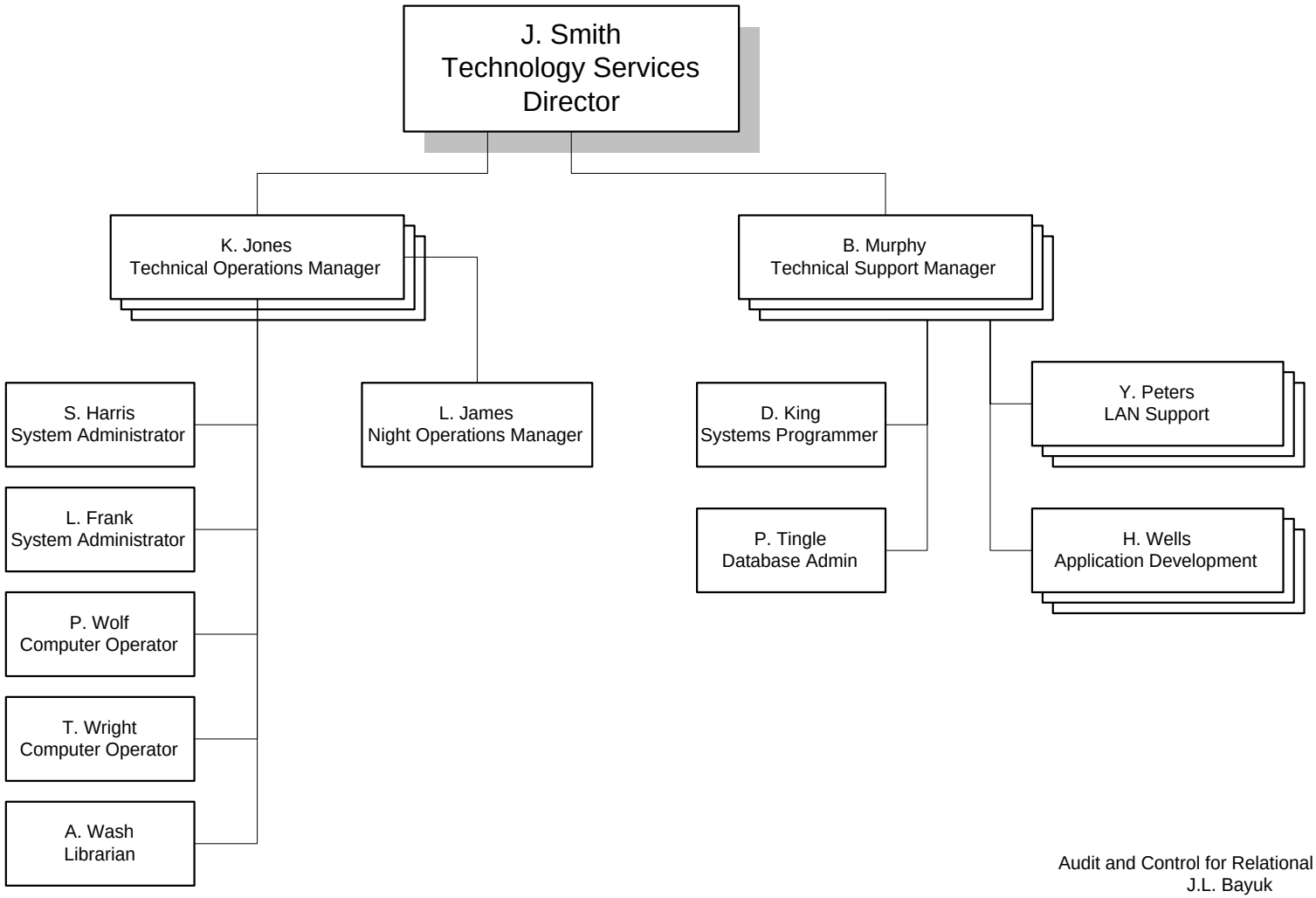
- DS: Audit data access
- SA: Audit data access and failed access attempts
- SA: Audit DBMS configuration
- SA: Maintain integrity of audit trail
- DBA: Record changes to database structure
  - Detection of incidents with performance impact
  - Periodically provide list of auhorized users to data steward

Segregation of Duties

RECOVERY:

- DBA: Develop “back-out scenarios” for database management system and/or database schema changes
- DBA: Plan and automate database backup and recovery mechanisms
- DS: Manage tests of business recovery plans

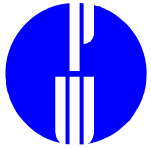
XYZ Corporation
Technology Services Division
Organization Chart
January 15, 1997



Audit and Control for Relational Database
J.L. Bayuk
Organizational Structure Exercise

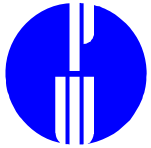
Database Administrator Example Job Description

- Create and maintain hardware and software requirements for data storage and retrieval
- Install and maintain production, assurance, and development databases
- Maintain list of active databases, remove inactive databases
- Automate DBMS startup and shutdown
- Monitor and analyze database management system performance
- Resolve database-related production system problems



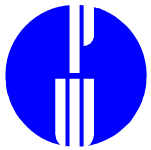
Caveats for Outsourcing

- Like system administrators, DBAs find it convenient to give all databases the same administrative passwords. This practice is often extended to entire vendor organizations.
- Backup requirements are often assumed to be daily rather than by transaction, batch, or hourly. Recovery times are correspondingly long.
- Security requirements must be readily available and specified by contract.



3. Security Mechanisms for RDBMS

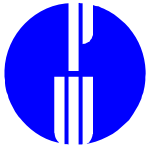
Prevention
Detection
Recovery



Prevention

Problems

- Standard installation contain generic passwords
- Applications embed security in code rather than database
- Non-application-controlled database accesscan result in corruption of transaction data
- Direct access to DBMS defeats application controls
- Database management systems transmit all transactions, data, user IDs and passwords in cleartext
- Network analysis (sniffer) software



Prevention

Solutions

- Changing passwords
- Groups and Roles
- Application Handshakes
- Password Masking
- Product Profiles
- Authentication Tools
- Encryption Tools

Prevention through Changing passwords

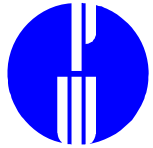
Product	DB ID	Password
Oracle	sys	change_on_install
Oracle	system	manager
Oracle	scott	tiger
Sybase	sa	<none on original install>
DB2	ibm	ibm
Peoplesoft	sysadm	sysadm
SAP	sap	sapr3
Summit	summit	summit

UNIX Ids - password usually user name: i.e.: username: ingres, password: ingres

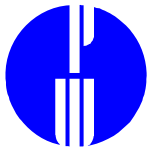
Safeguards for Generic IDs

- Always change initial passwords.
- Wherever possible, change the name of the account or disable the privileged account and grant the necessary privileges to an account of a different name.

Prevention through Groups and Role Assignments



- Sybase, Oracle, and MS-SQL allow users to be assigned to groups.
  - Sybase predefined roles are:
    - sa_role = database management system administrator
    - dbo_role = full control over indidivual database
    - sso_role = manages logins, audits
    - oper_role,navigator_role,replication_role = subadmin
  - Oracle roles (groups) may be assigned any set of permissions and users be assigned to multiple roles.
- Informix allows groups only at operating system level to determine Informix access
- Application privilege assignments should not be expected to correspond to DBMS group assignments.



Prevention through Application Handshakes

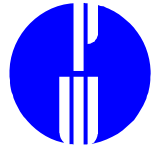
Stored procedure key-based authentication

- Prevents users from running stored procedures from a command line

Implementations

- Code conditional into procedure or trigger that forbids execution unless it is passed a secret key from the application
- Code conditional into procedure or trigger that forbids execution if process ID does not = application name.

Prevention through Profiles



ORACLE Product User Profile
Can be used to limit ad-hoc access by product
Must be configured for ALL products

select * from sys.product_user_profile;

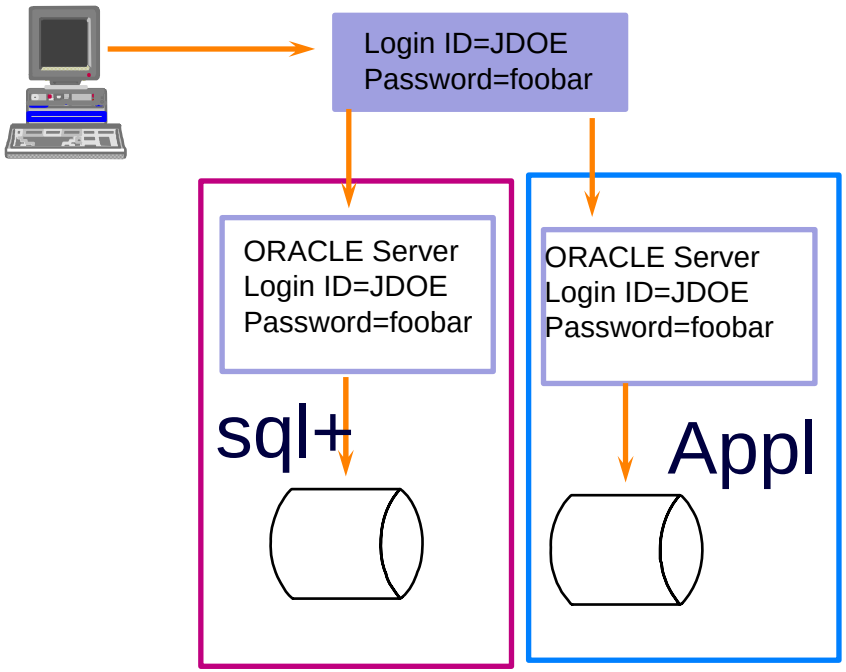
select * from sys.product_user_profile;

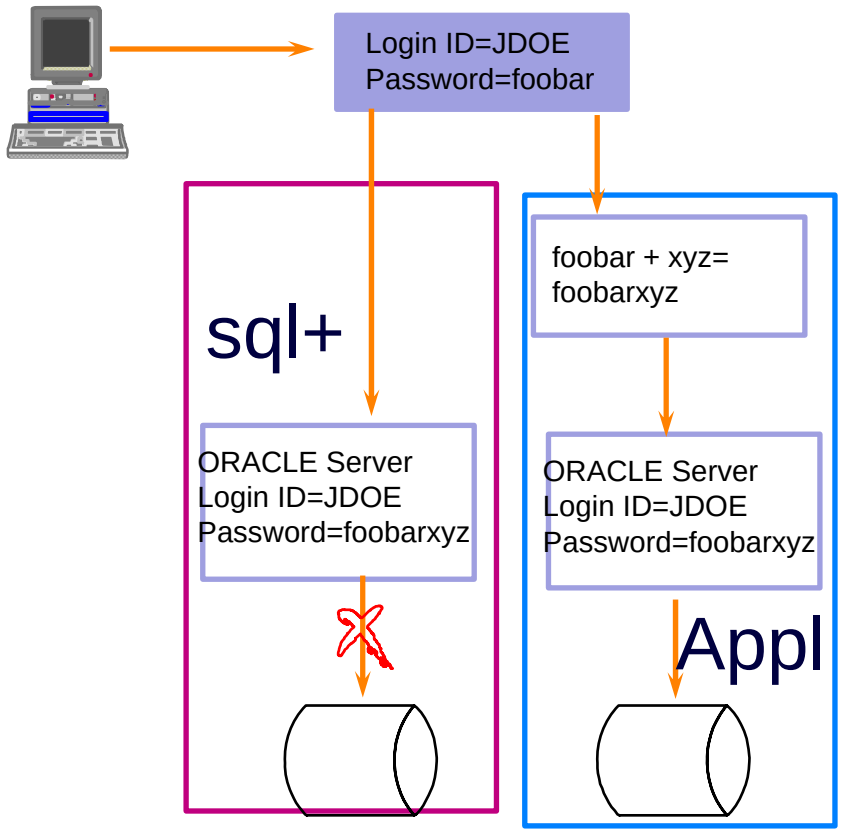
PRODUCT	USERID	ATTRIBUTE	SCOPE	NUMERIC VALUE	CHAR VALUE	DATE VALUE
SQL*Plus	JDOE	GRANT			DISABLE	
SQL*Plus	JSMITH	AUDIT			D DISABLE	
SQL*Plus	JSMITH	SET ROLE			D DISABLE	
SQL*Plus	%	INSERT			D DISABLE	
SQL*Plus	%	UPDATE			D DISABLE	
SQL*Plus	%	DELETE			D DISABLE	
SQL*Plus	%	SELECT			D DISABLE	
SQL*Plus	ROLES				D CLERK	
SQL*Plus	ROLES				ADMIN	

Prevention through Password Masking

Password Masking

Protects from ad-hoc access to stored procedures and database tables





Prevention through Authentication Tools

Solutions:

- Single sign on
- Hand-held authentication
- Biometrics

Single Sign On

Pros

- User convenience

Cons

- Expensive
- Considerable administrative overhead

Tools

- SeOs
- Boks
- ESM

Hand-held authentication

Pros

- May minimize network eavesdropping threat
- Disallows shared passwords

Cons

- User annoyance
- Expensive
- Inventory constraints
- Considerable administrative overhead

Tools

- SKEY
- SecurID

Note: Challenge Response algorithms are stronger than simple tokens

Biometrics

Pros

- May minimize network eavesdropping threat
- Disallows shared passwords

Cons

- Expensive
- Considerable administrative overhead
- Implementation may not address network vulnerabilities

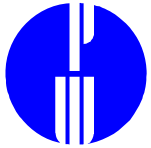
Tools

- Identix
- NR-Id

Prevention through Encryption

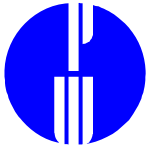
Solutions:

- Hardware Level Encryption
- Network Level Encryption
- Database Level Encryption
- Application Level Encryption



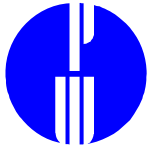
Hardware Level Encryption

- Pros
  - Speed
  - No Key Exchange
- Cons
  - Expensive
- Tools
  - Jones Futurex
  - Lucent
  - BorderGuard



Database Level Encryption

- Pros
  - Transparent to application program
- Cons
  - Semi-configurable (checksum <> datastream)
  - Performance impact
  - Key management issue
- Tools
  - Oracle SQL-Net
  - Sybase password transmittal encryption option
    - between Sybase servers



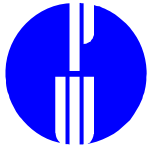
Application Level Encryption

Pros
- Highly configurable
- Transparent to database

Cons
- Development intensive
- Performance impact
- Key management issues

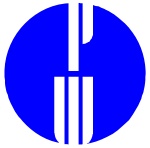
Tools
- DCE
- RSA
- PGP

Prevention: Best Practices



- Change all generic passwords
- Use group or role security whenever possible
- Implement all password complexity and aging features of the DBMS
- Do not allow direct modifications to database tables
- Control report generation as you control data entry
- Encrypt all DBMS-related network traffic

Detection: DBMS Audit Systems



Problems

- Default configuration has all auditing disabled
- Comprehensive audit requires considerable CPU and storage

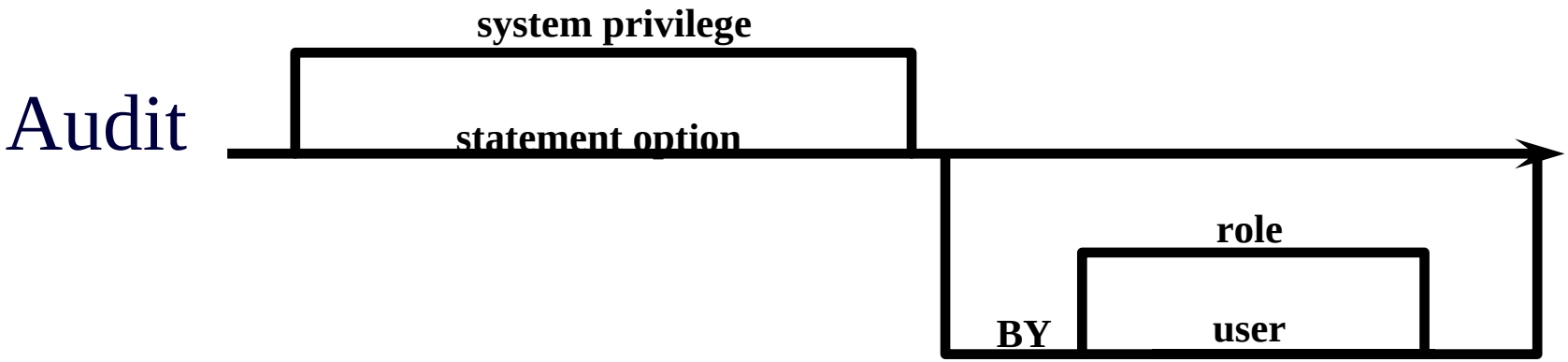
Solutions

- System-level audits
- Object-level audits
- Statement-level audits

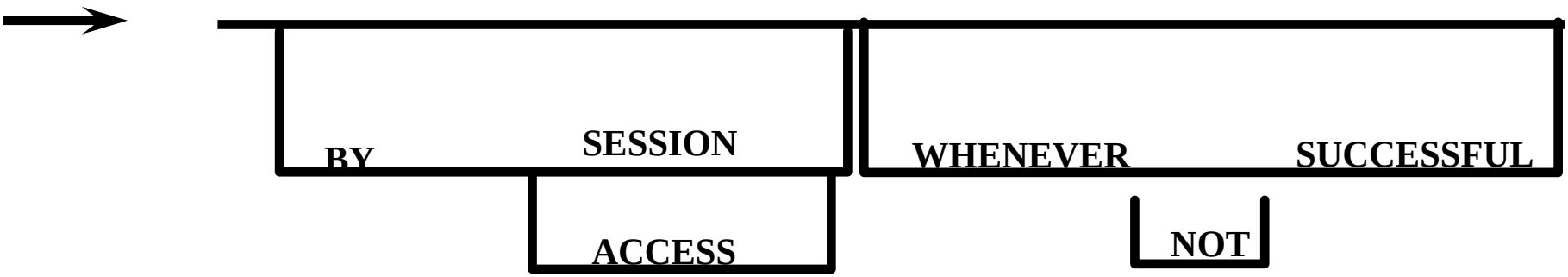
Levels of DBMS Audit

- System
  - Audits of activity other than data access
- Object
  - Audits that are recorded whenever a given object is accessed
- Statement
  - Audits record commands issued (not necessarily that they were issued successfully)

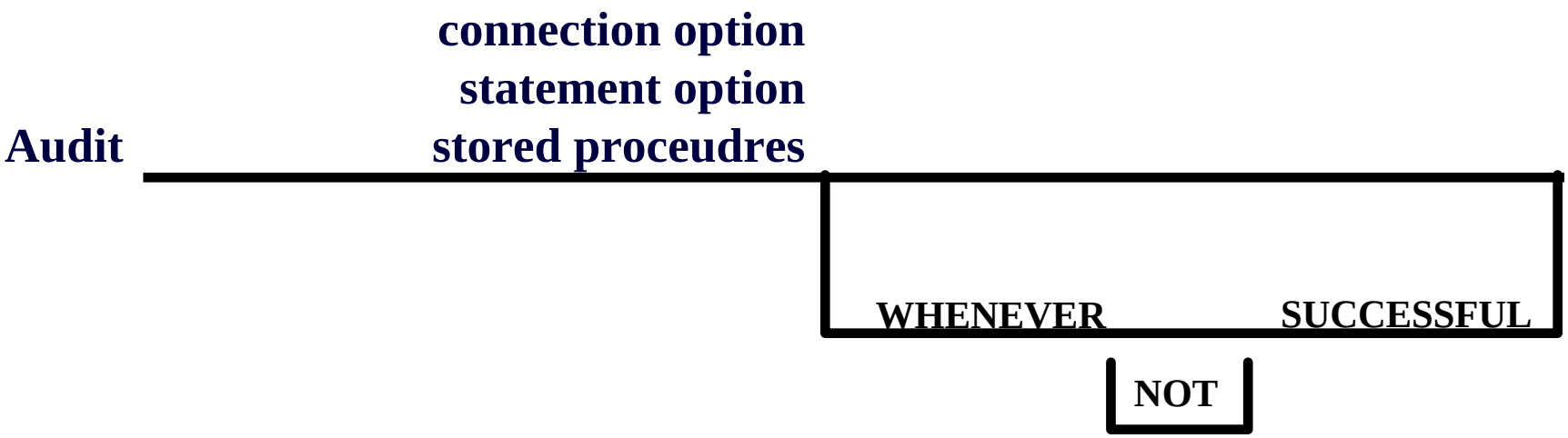
Detection Options: ORACLE



Audit <privilege> on Object



Detection Options: Sybase

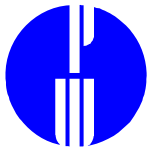


ALSO:

All commands issues by SA, SSO,or all users

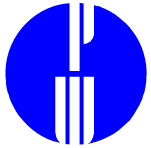
Server boots

Detection: Best Practices



- Audit all commands entered by the DBA
- Audit all commands entered by users with direct access to data
- Store the audit trail at the operating system level if supported, and ensure DBA does not have superuser password
- Automate alerting based on the audit log

DBMS Recovery



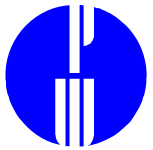
Problems

- Database operation relies on operating system and application configuration
- Operating system backup may not cover most recent database transactions

Solutions

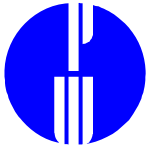
- Operating System backup
- Application backup
- Data file backup
- Transaction-based backup

Transaction-based backup



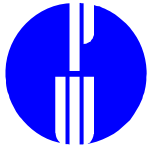
- Database transactions are written to a separate file in addition to the database itself: a transaction log.
- If the database is corrupted, transaction logs may be applied to a database backup.
- Data is restored to the time of the last available transaction log.

Transactions Logs



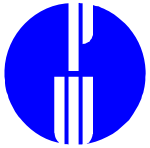
- Ensure the transaction log is updated well within the minimum recovery time interval required.
- Periodically back up the transaction log
- Ensure that the transaction log is backed up before it is truncated.

Recovery: Best Practices



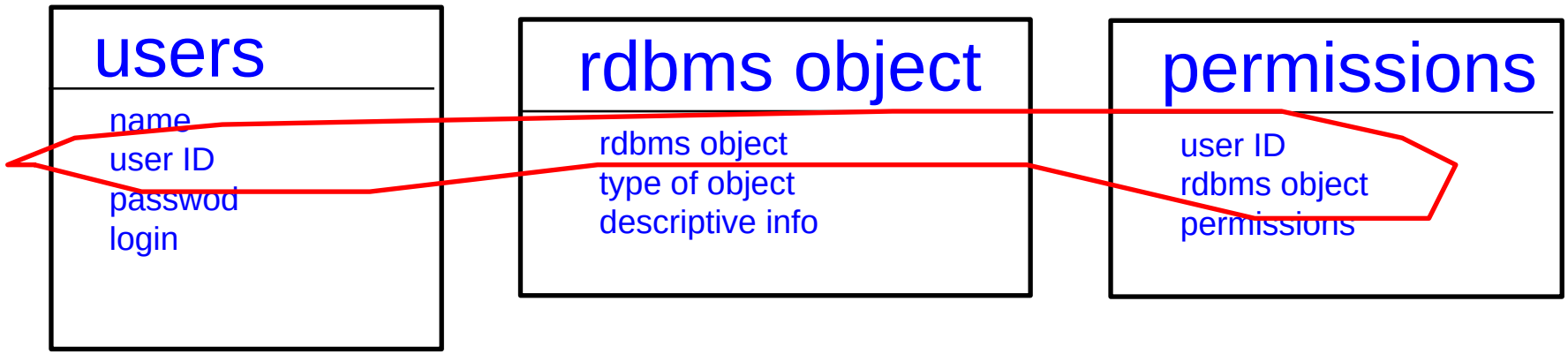
- Transaction-based backup
- Copy backup to another server in near real time
- Allow no transactional updates to backup server
- Integrate DBMS recovery strategy into Business Recovery Plan

4. Structured Query Language



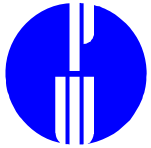
Relational Data
Security-Related Tables
Example SQL Queries

Reminder: INFORMATION ON ACCESS TO A RELATIONAL DATABASE:

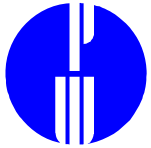


IS STORED JUST LIKE THE RELATIONAL DATA

Database Objects



- Tables
- Stored procedures
- Rules
- Triggers
- Defaults

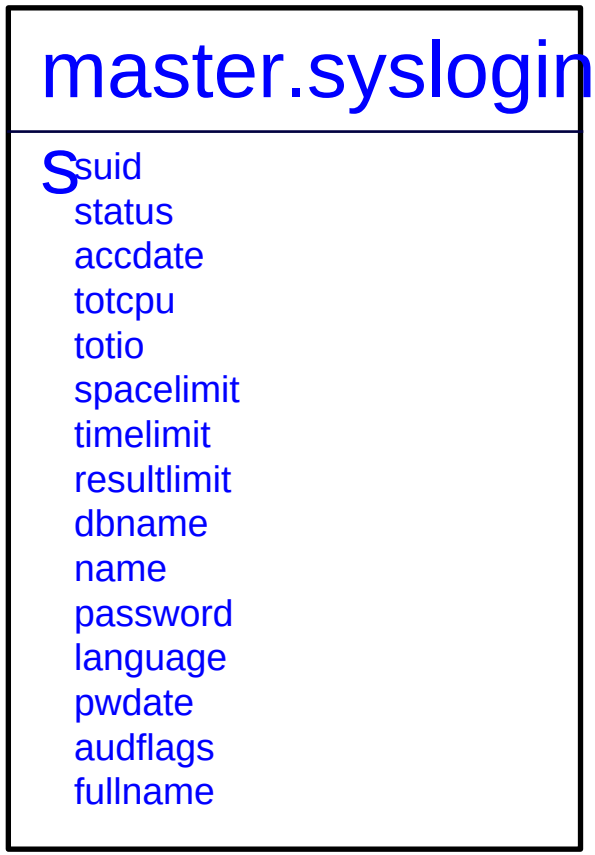


Database Permissions

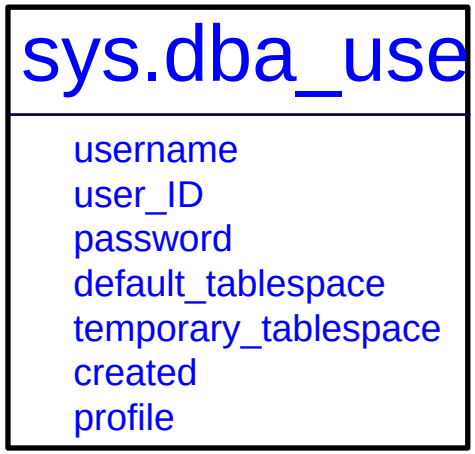
Select
Insert
Update
Delete
Execute
Views (column security)

Case Study: Sybase and Oracle

Sybase table of users: syslogins
sys.dba_users

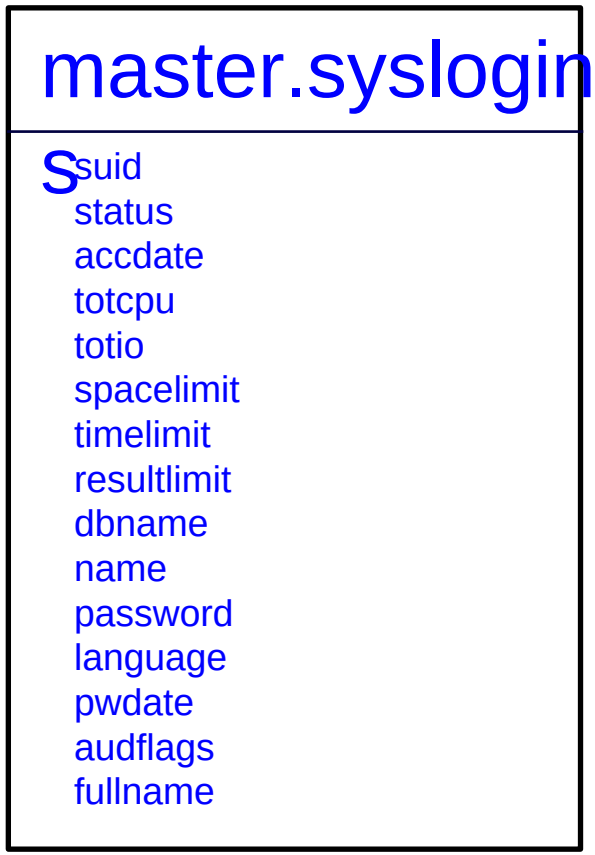


Oracle table of users:

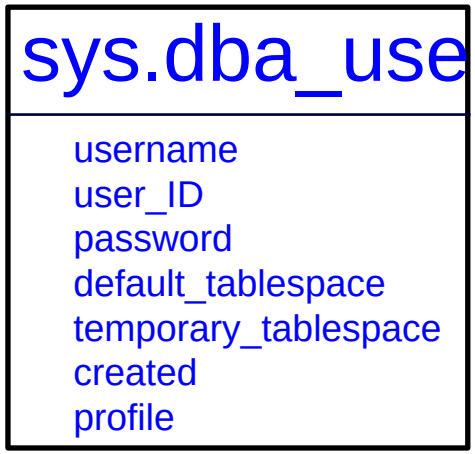


Case Study: Sybase and Oracle

Sybase table of users: syslogins
sys.dba_users

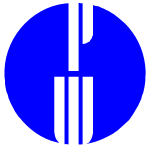


Oracle table of users:



Question:
How to use an RDBMS to list the users?

Case Study: Sybase and Oracle



Sybase table of users: syslogins
sys.dba_users

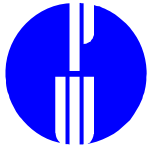
master.syslogin
suid
status
accdate
totcpu
totio
spacelimit
timelimit
resultlimit
dbname
name
password
language
pwdate
audflags
fullname

Oracle table of users:

sys.dba_users
username
user_ID
password
default_tablespace
temporary_tablespace
created
profile

Question:
How to use an RDBMS to list the users?

ANSWER: SQL



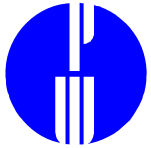
SQL (Structured Query Language)

Select Statement

select **X** from **Y**

X=column name of data item

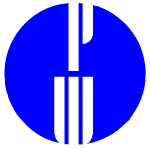
Y=table name



Exercise:

List users in Sybase and Oracle

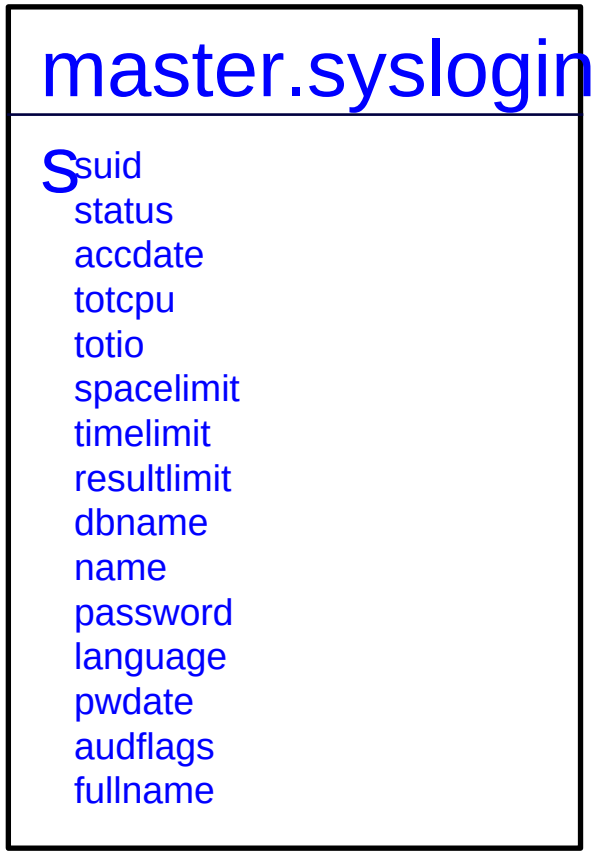
(take 2-3 minutes)



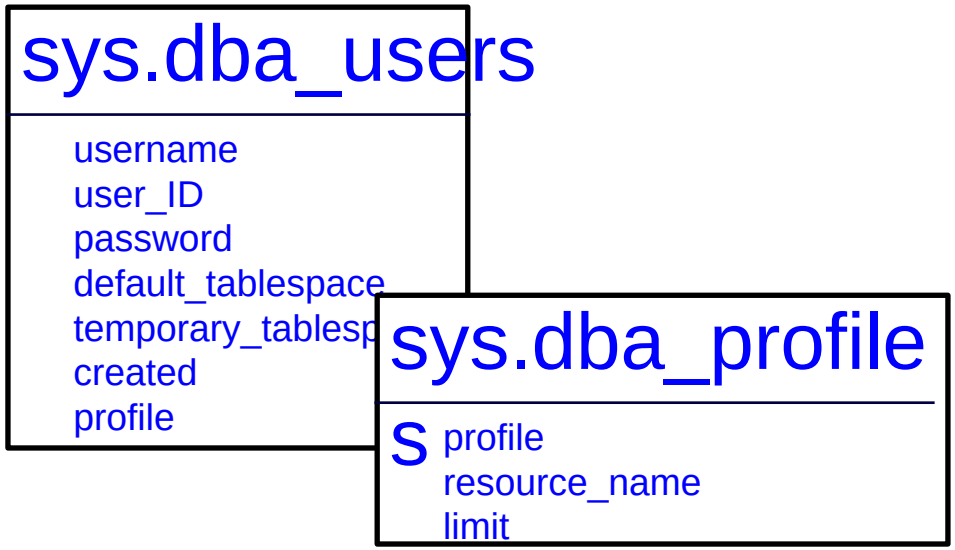
Exercise Answers:

Case Study: Sybase and Oracle

Sybase table of users: syslogins
sys.dba_users



Oracle table of users:



Question:
How to use an RDBMS to list space constraints on

SQL (Structured Query Language)

More about the Select Statement

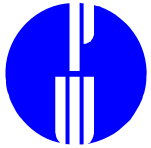
select **Y.X** from **Y,Z where Y.X=Z.X**

Y=table name

Z=table name

X=column name of data item where the
value of the data is the same in both tables **Y** and **Z**

Y.X = the column **X** in the table **Y**
Z.X = the column **X** in the table **Z**

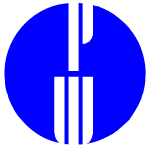


Exercise:

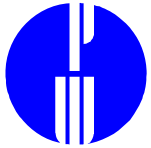
List the spacelimits on users in Sybase and Oracle.

Hint: In Oracle, spacelimits are stored in the user's profile. The resource name for the Oracle spacelimit is "PRIVATE_SGA".

(take 3-5 minutes)



Exercise Answers:



Security-related info in a DBMS:

Prevention:

user names, groups, permissions granted....

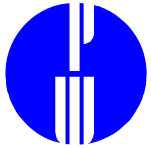
Detection:

audit trails, configuration parameters.....

Recovery:

recovery mechanisms, dbms utilities.....

5. Automated Processing



Scheduling
File Transfer
DBMS Monitoring

Scheduling Tools

In the DBMS environment, used for:

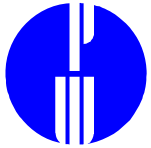
- dumping database raw partitions to disk for backup
- reading in batched input data
- generating and distributing reports or data feeds
- monitoring database integrity or security

Where access to DBMS is required, must be configured with database user privileges.

Scheduling Tool Features

- Start jobs recurring periodically or one-time in future
- Allow use to be restricted to certain operating system users
- May run a job with any given operating system id

File Transfer



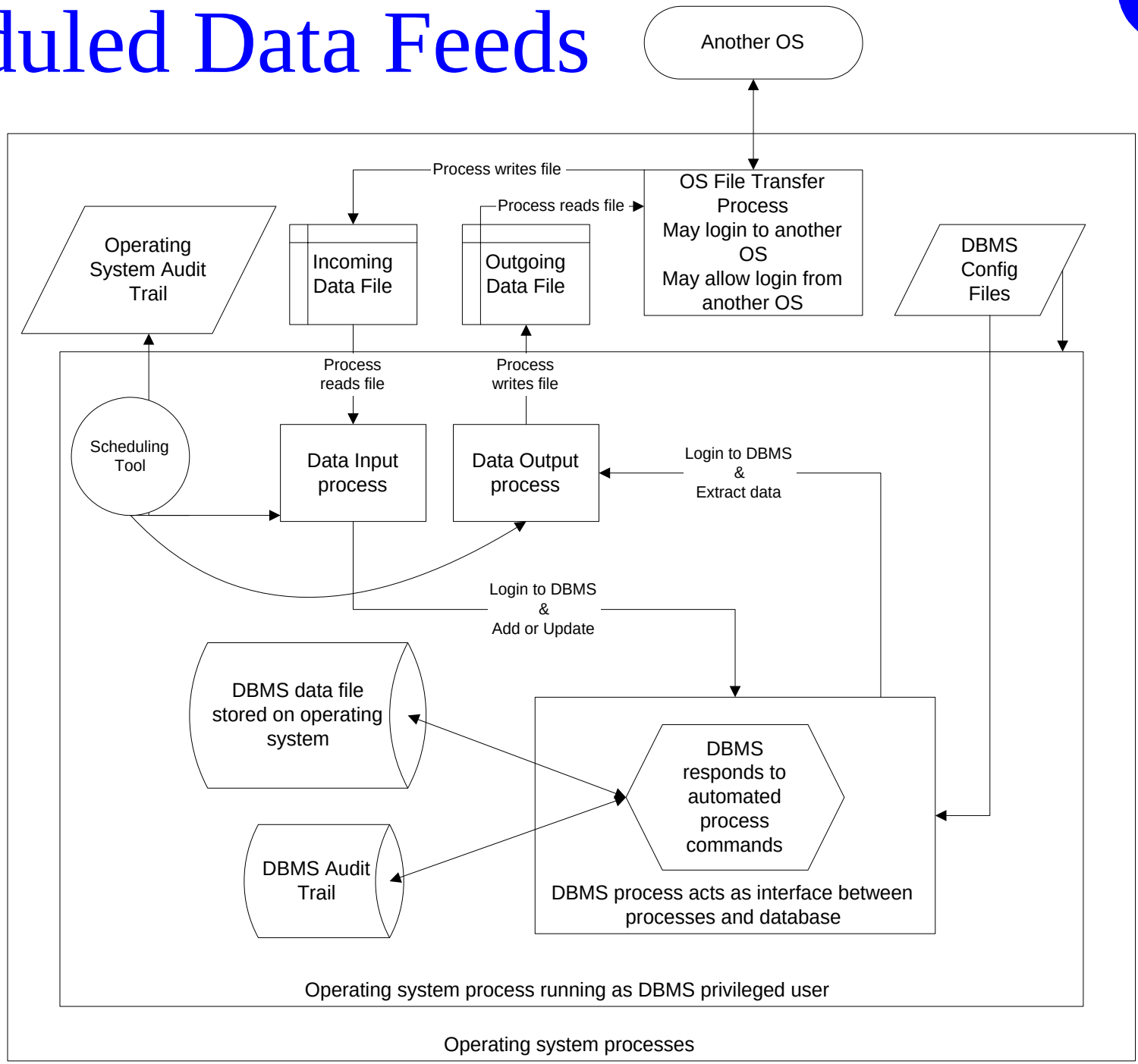
	Passive	Active
Scheduled	remote machine logs in at specific time	process logs in to remote machine at specific time
Polling	remote machine logs in periodically to check for files	process logs in to remote machine periodically

File Transfer

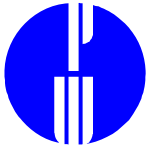
Amounts to batch data entry

Same controls apply

Scheduled Data Feeds



UNIX Scheduling Tools



- cron

  cron “tables” allow users to set up jobs to run daily, weekly or monthly

- at

  at commands allow a user to submit jobd to be run at a given future time

restrictions:

- cron(at).allow - only users in this file may use cron
- cron(at).deny - users in this file may not use cron (at) -all others users may (unless restructed via cron(at).allow)
- if neither file exists, only root may use cron (at)

Monitoring Tools

Operating system monitoring tools

- can be configured to verify configuration of database-specific operating system files
- can be used to monitor critical database processes

Network monitoring tools

- can be configured to check for unusual remote database activity

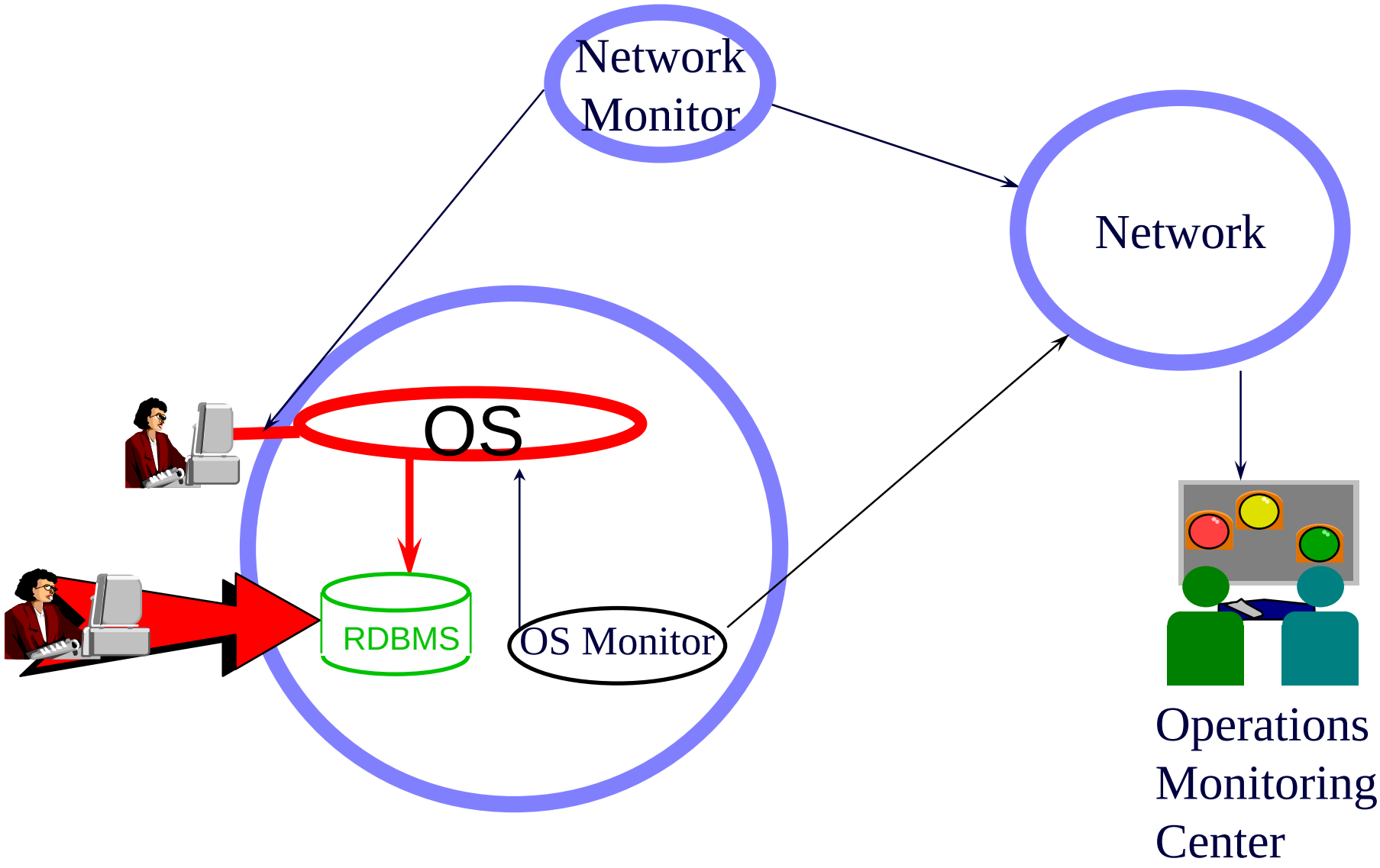
Database management tools

- can be configured to check for changes to database security

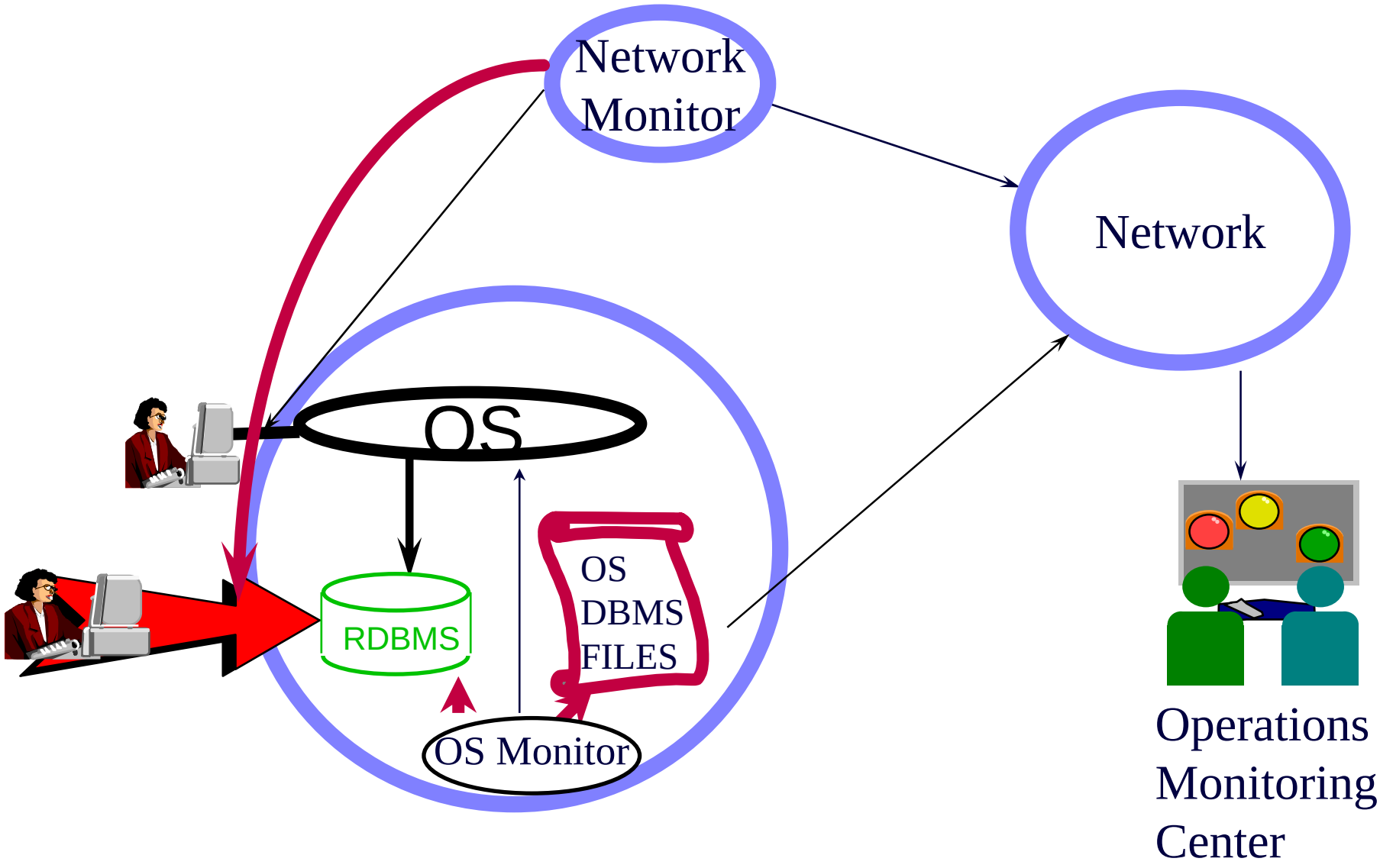
Network management tools

- can be configured to poll or receive alerts from operating system, network, and database tools

Typical Operations Monitoring



Integrating DBMS Monitoring



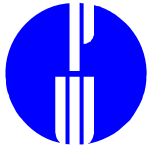
Configuration Techniques

- OS Monitor may be configured to:
  - detect changes in start-up files
  - detect an interruption in the programs that provide database management system services
- Network Monitor may be configured to:
  - monitor patterns of network access to database management system
  - detect multiple failed access attempts to database management system

Information on Tools

- ISACA Journal Annual Buyer's Guide
  847-253-1545
  publication@isaca.org
  www.isaca.org
- Computer Security Institute (CSI) Computer Security Products Buyer's Guide
  415-905-2626
  csi@mfi.com
  www.gocsi.com
- InfoSecurity News
  508-879-9792
  isn@misti.ccmail.compuserve.com
  www.infosecnews.com/isn

6. RDBMS Management

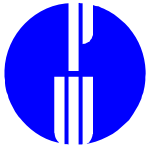


Information Classification Sample Policies

Information Classification

- Definition of “proprietary”
- If appropriate, definition of other levels of classification
- Provides guidelines for identifying classified information

Identifying proprietary information



- Focused on data, not on platform or application
- Should follow guidelines for identifying classified information
- Requires awareness of legal and regulatory requirements

Labeling proprietary information

- Phrasing requires legal involvement
- Consider implementation issues
  - Standard markings
  - Screen warnings
  - Automated report labels

Controls on classified information

- generation
- storage
- retrieval
- transmission
- distribution
- retention
- disposal
- change of classification

Responsibilities with respect to each level of classification

- Classify - Management controls
- Identify - Data Steward
- Label - Application developers, system, network, and database administrators
- Control - All of the above

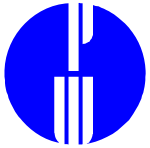
Policy

Without policy, no person is responsible for controlling information assets or is accountable for not having done so.

Awareness

A person who is not aware of an database policy is not necessarily accountable for violating it.

Administration



To achieve assurance that policy is being followed uniformly throughout the organization, database management must also address *how* policy is to be realized through user and database administration.

Monitoring

If guidelines on how to control database configuration are followed, then these will also provide guidelines on how to recognize a security or performance incident.

Compliance

A database management process requires methods to ensure that known vulnerabilities are closed and open issues are resolved.

Strategy

A foresighted database management process will ensure that database management stays abreast of changes in the information technology environment.