RACF Overview

Leanne Wilson

VERTALI

Introduction

Leanne Wilson

Senior Security Consultant

Worked on mainframes for 12 years

Worked on many security-based projects

Also worked as an Information Security Manager concerned with GRC.

AGENDA

- RACF Overview
- User & Group Profiles
- Dataset & General Resource Profiles
- Access Granted ! Access Denied !
- Summary

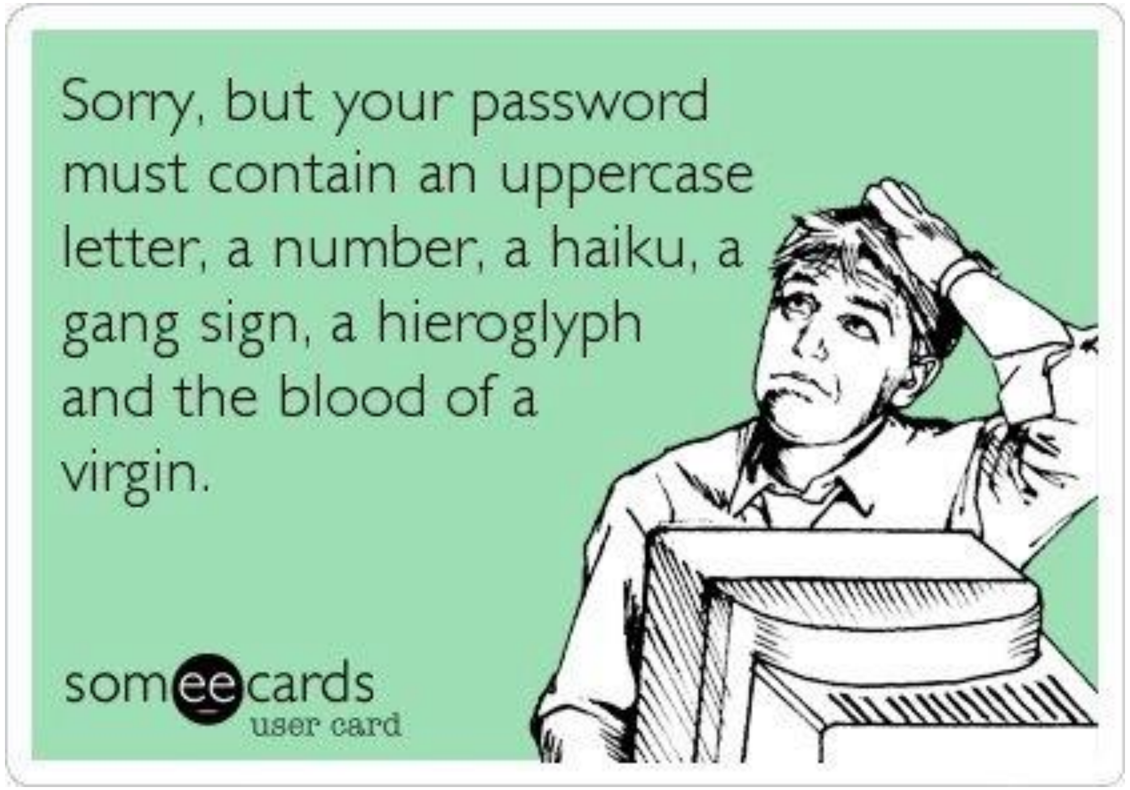
Overview

What is security?

The protection of data from unauthorised*:*

- Destruction
- Modification
- Disclosure
- Use

Whether accidental or intentional!

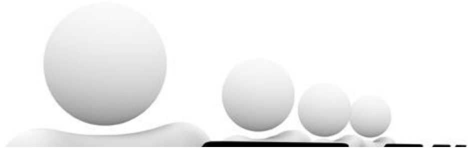


Sorry, but your password must contain an uppercase letter, a number, a haiku, a gang sign, a hieroglyph and the blood of a virgin.

What security do we need?

Protect the data & resources

Control the users



Isolate the network

R ESOURCE

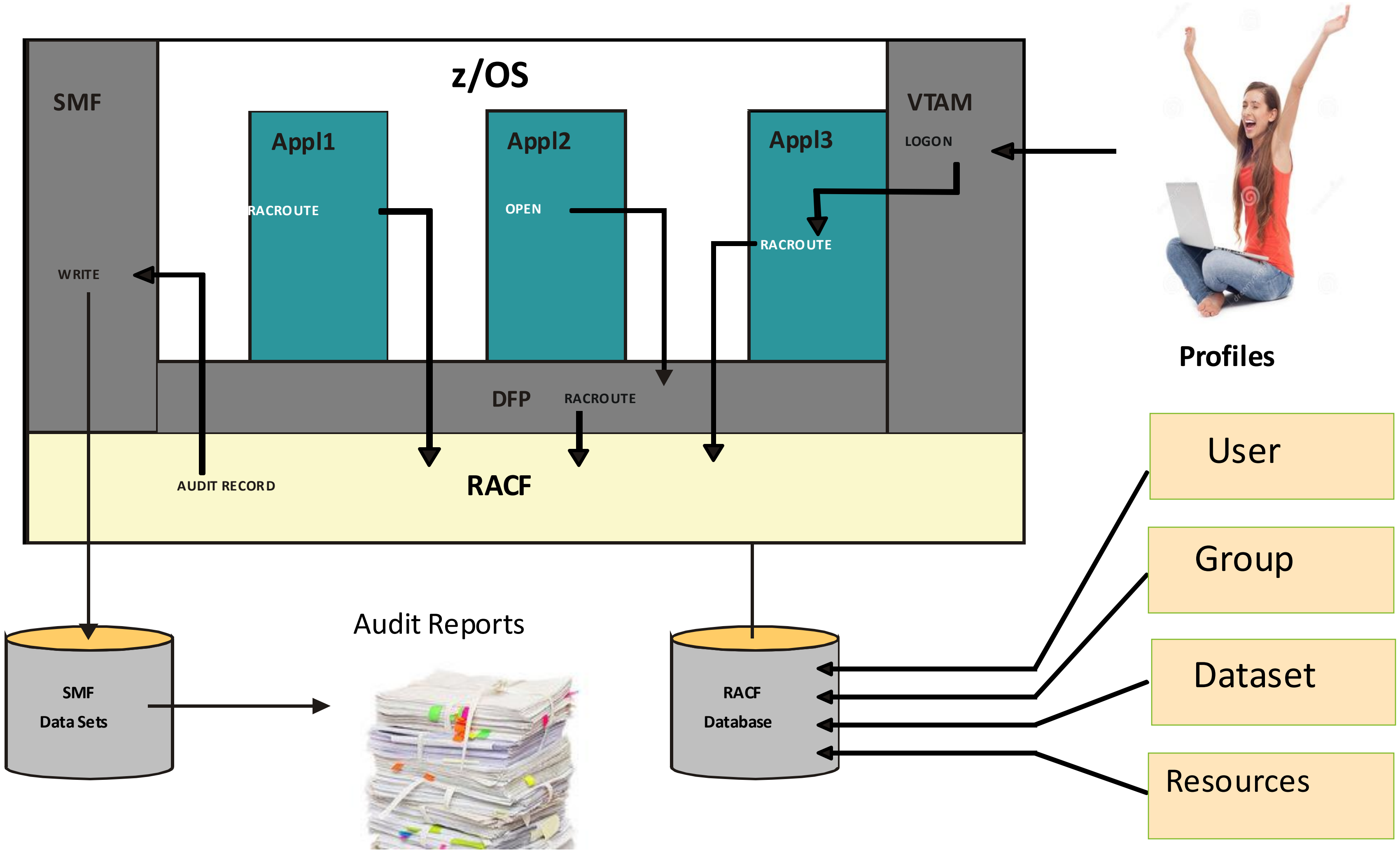
A ACCESS

C ONTROL

F ACILITY

- IBM's software product that provides security services for z/OS
- RACF consists of a database and an extensive set of programs that manage and query it
- Includes a primary database(s) and optional on-line backup database(s)
- The database contains records called "Profiles" that are used to govern security
- Using RACF doesn’t make the mainframe secure; it allows us to make it secure!

How RACF works



z/OS

SMF

WRITE

Appl1

RACROUTE

Appl2

OPEN

Appl3

RACROUTE

VTAM

LOGON

DFP

RACROUTE

AUDIT RECORD

RACF

Profiles

User

Group

Dataset

Resources

SMF

Data Sets

Audit Reports

RACF

Database

How Can RACF Help?

MARVEL
AVENGERS ASSEMBLE
MARVEL.com

User Profiles

Group Profiles

User Profiles

Dataset Profiles

Resource Profiles

Dataset Profiles

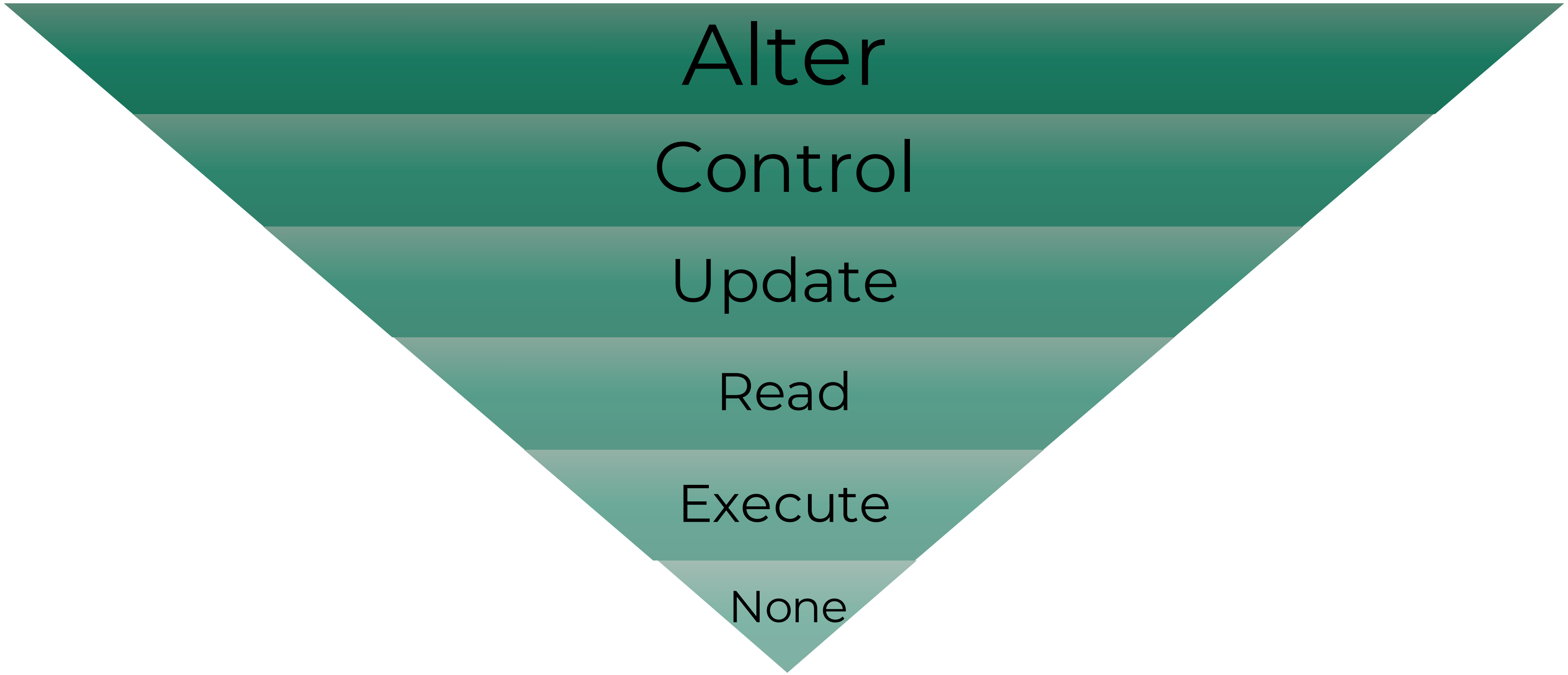
Resource Profiles

TSGLW.JCL.**

Avengers	READ
Thor	UPDATE
Loki	ALTER

Class UNIXPRIV
SUPERUSER.FILESYS.CHOWN

Avengers	ALTER
Thor	UPDATE
Loki	READ



Alter

Control

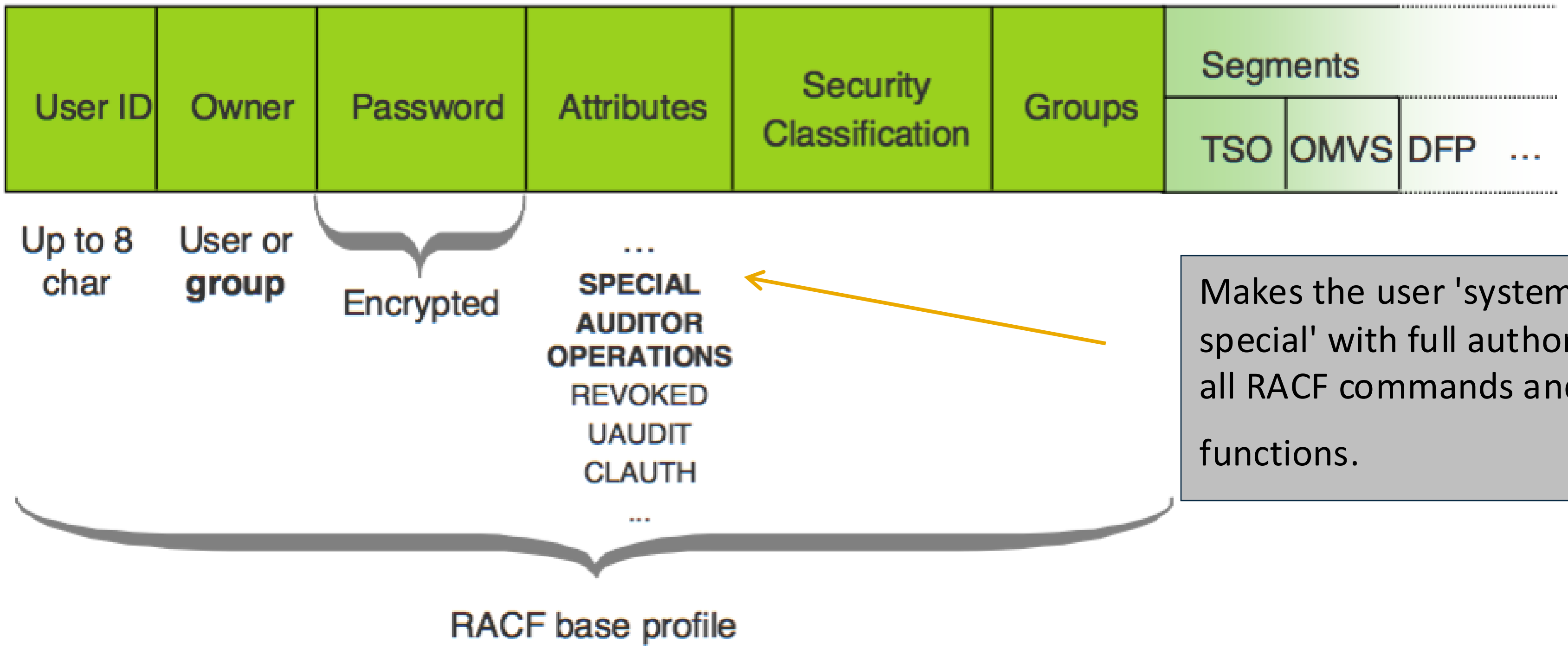
Update

Read

Execute

None

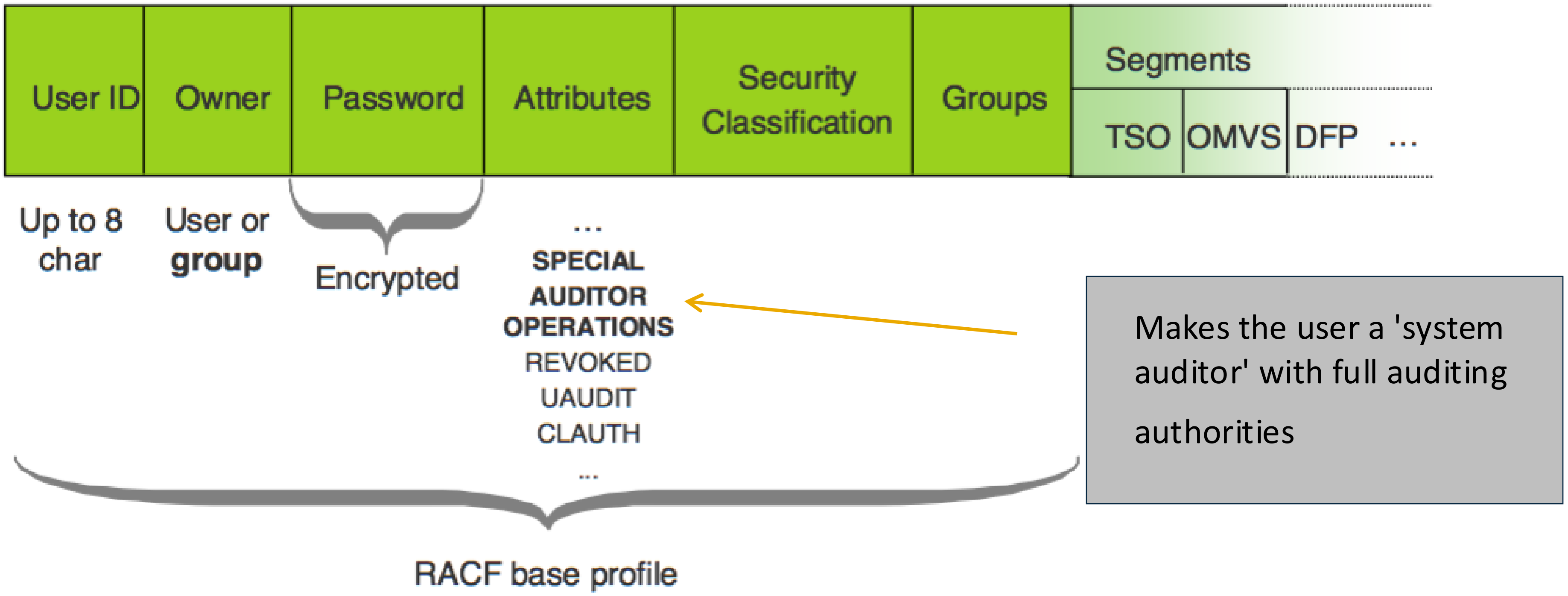
User Profiles



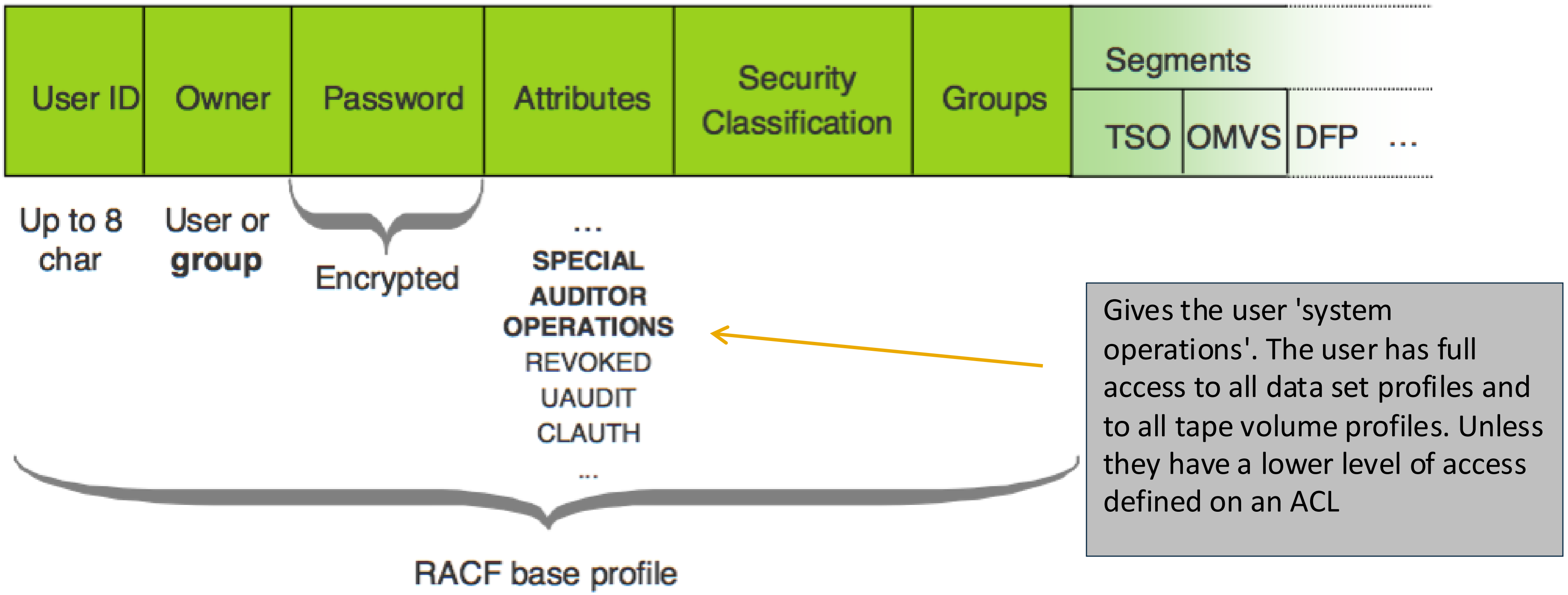
User ID	Owner	Password	Attributes	Security Classification	Groups	Segments
						TSO OMVS DFP ...
Up to 8 char	User or **group**	Encrypted	... **SPECIAL** **AUDITOR** **OPERATIONS** REVOKED UAUDIT CLAUTH ...			

RACF base profile

Makes the user 'system special' with full authority to all RACF commands and functions.



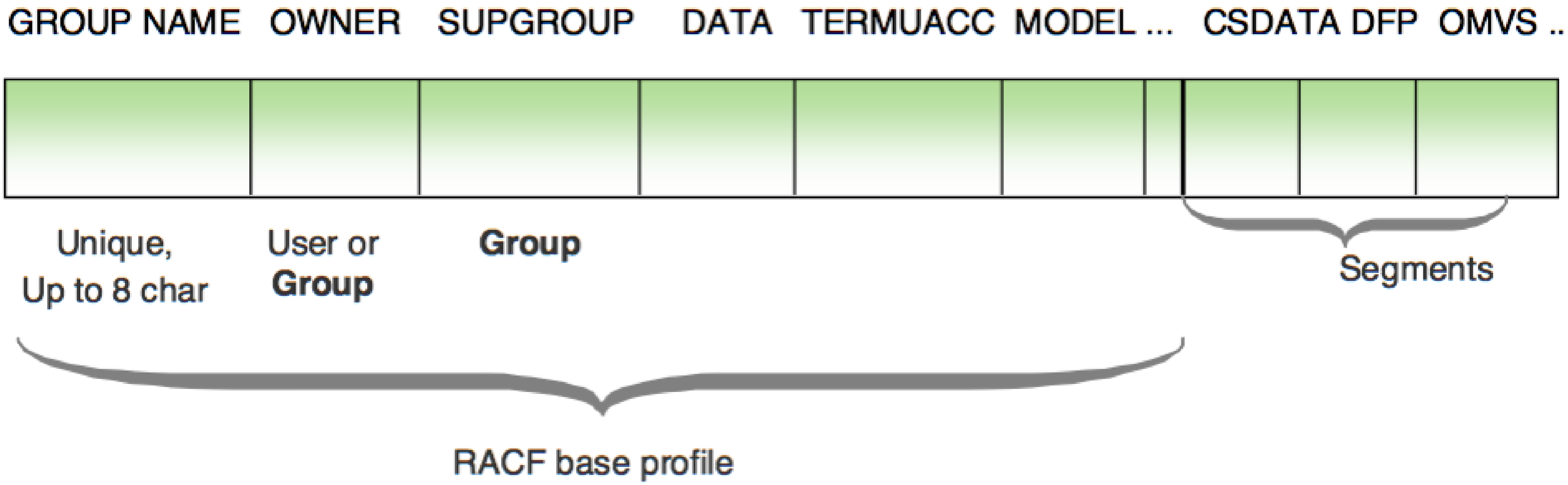
Makes the user a 'system auditor' with full auditing authorities



Gives the user 'system operations'. The user has full access to all data set profiles and to all tape volume profiles. Unless they have a lower level of access defined on an ACL

Group Profiles

VERTALI



GROUP NAME OWNER SUPGROUP DATA TERMUACC MODEL ... CSDATA DFP OMVS ..

Unique,
Up to 8 char

User or
Group

Group

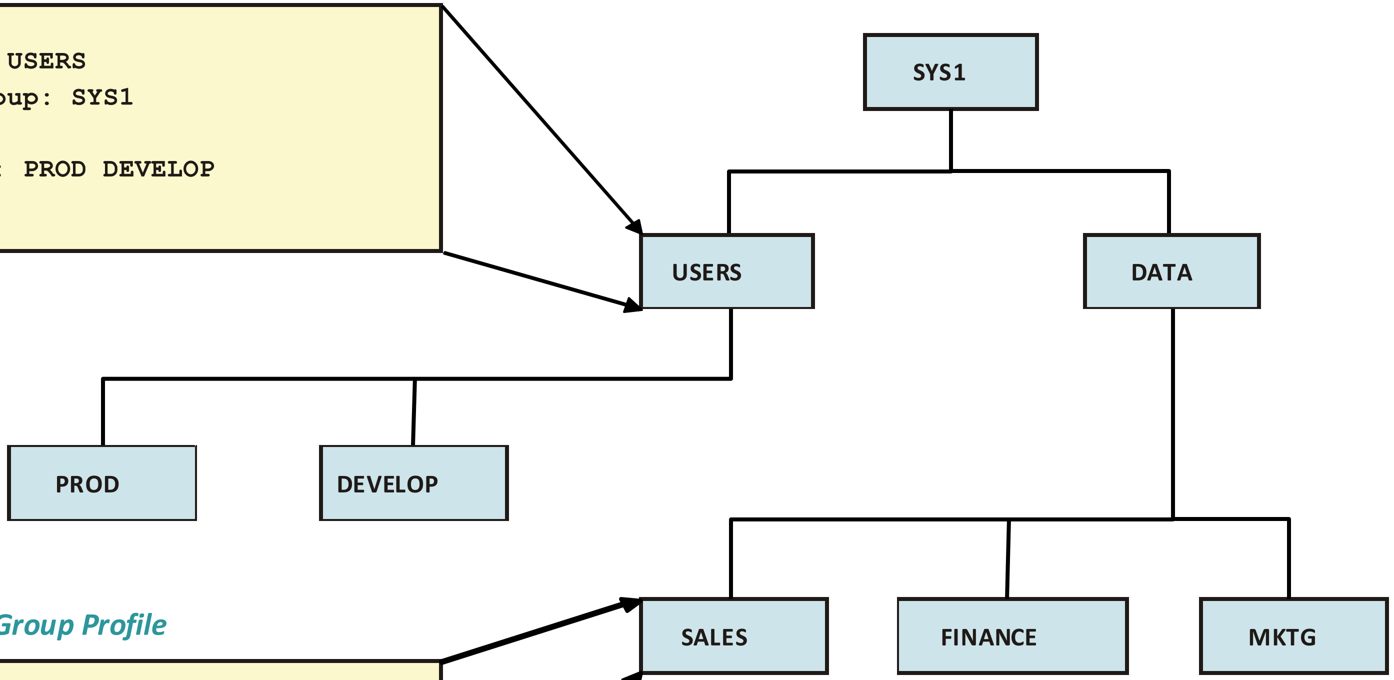
Segments

RACF base profile

What are groups?

USERS Group Profile

```
Group Name: USERS
Superior Group: SYS1
Owner: SYS1
Subgroup(s): PROD DEVELOP
Users: NONE
```



SALES Group Profile

```
Group Name: SALES
Superior Group: DATA
Owner: DATA
Subgroup(s): NONE
Users: NONE
```

Groups are stored as profiles

Groups provide the structure

Groups have a hierarchy

Grouping resources and users

Group resources together:

Used by the same users

Have the same owner

Are logically connected

Connected to the RACF group structure

Group users together:

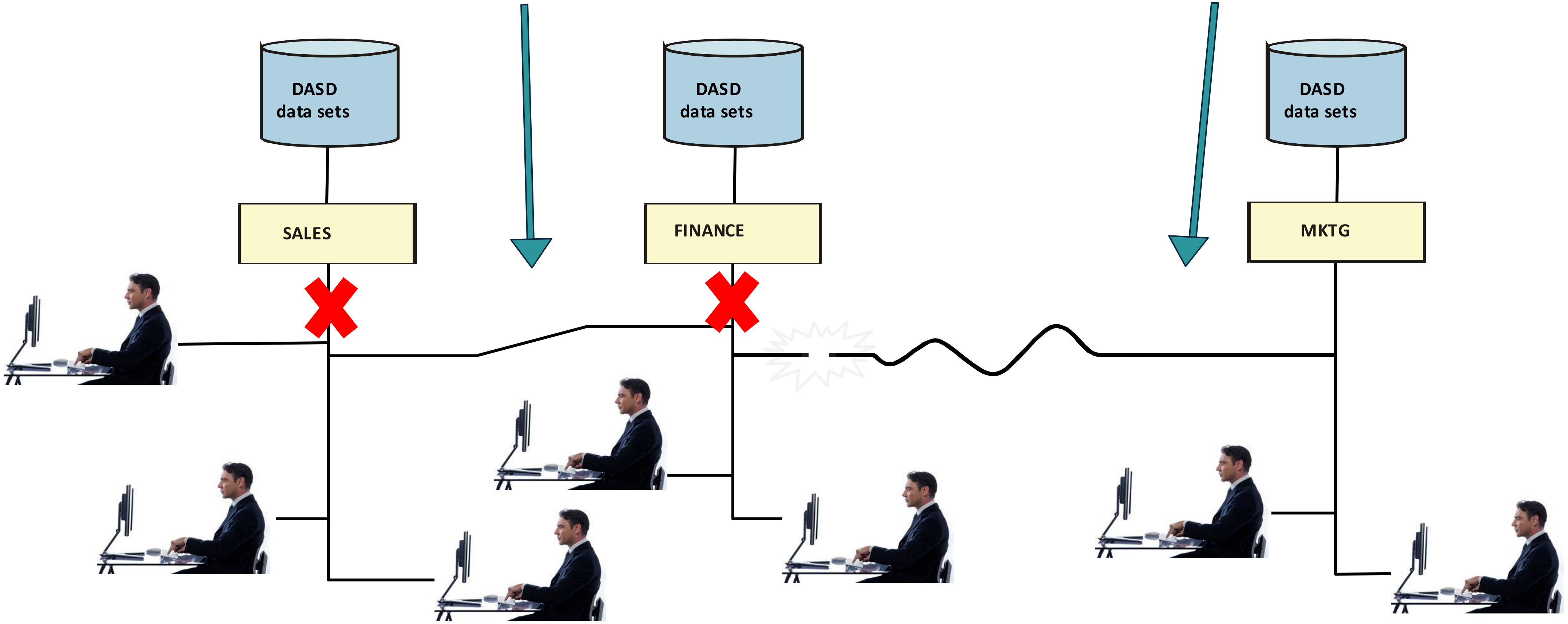
Using the same resources

Have the same manager

Belong to the same department

Do the same job

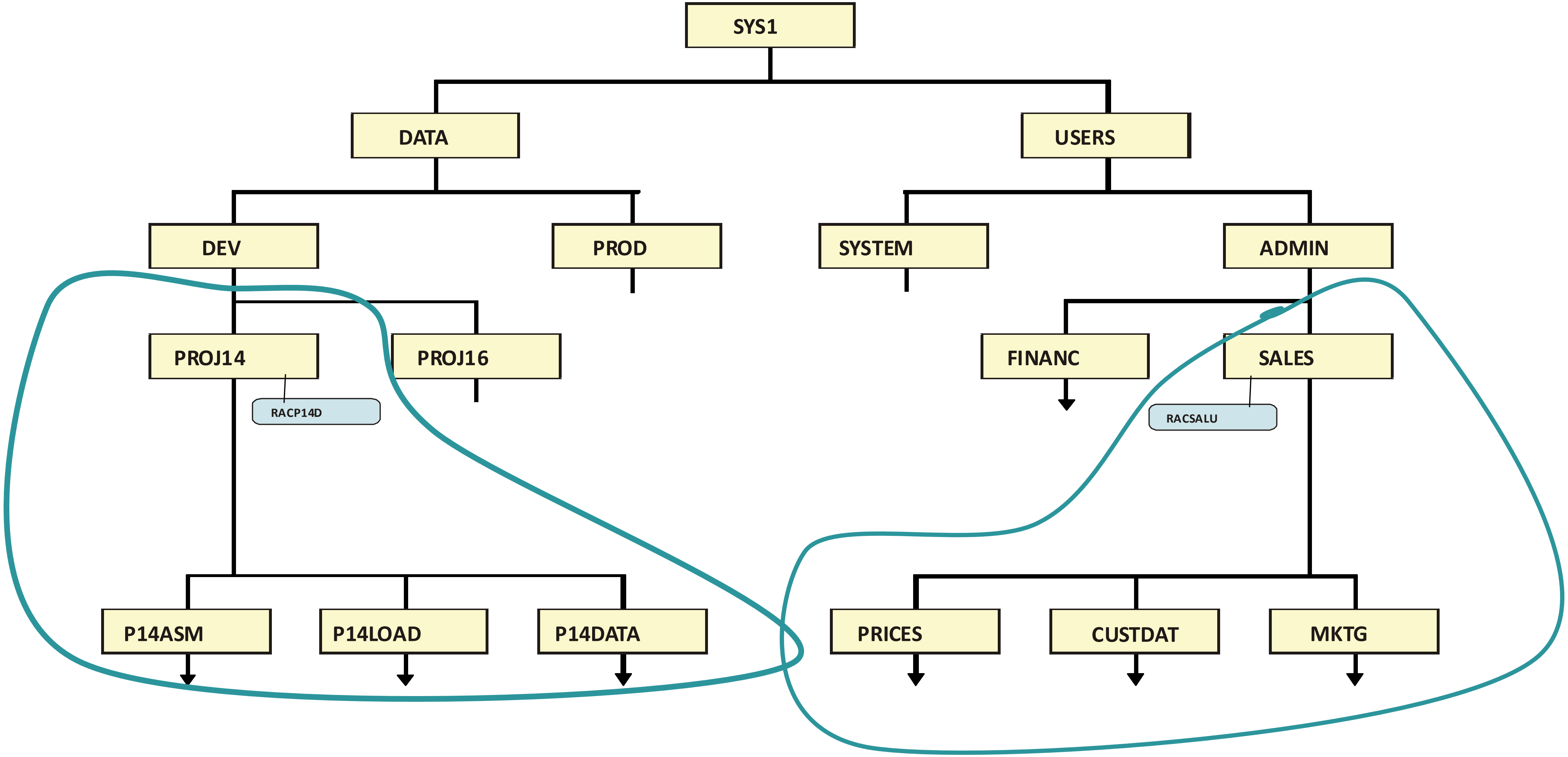
Users and groups



Users who are connected to multiple groups, get access to all resources to which the groups have access

A user who has been disconnected from a group immediately ceases to have access to group resources

Group Level Attributes



Dataset Profiles

VERTALI

Profile	Owner	UACC	Warning	Erase	Auditing	ACL	Segments
44 chars							....

RACF base profile

Discrete Profiles	Generic Profiles
Protects one dataset	Protects multiple datasets Use of 3 wildcard characters % , * , ** Use of ** requires EGN activated in SETROPTS
Not possible to create a discrete profile unless a data set of the same name already exists	A generic profile can be created even if no data set matching the name exists
If a data set protected by a discrete profile is deleted then RACF will unconditionally delete the profile	When a data set protected by a generic profile is deleted the profile is not

VERTALI

Generic Profiles

- TSGLW.J*.**
- TSGLW.J%.**

Discrete Profiles

- TSGLW.JCL.CNTL

All examples are listed as if EGN is activated

TSGLW.JCL.CNTL
TSGLW.JCL.CNTL.BACKUP
TSGLW.JA.WORK
TSGLW.JB.WORK.OLD

Generic wildcard characters:

% **Matches with any single character**
* **Matches with any number of characters in the qualifier**
** **Matches with any number of characters and qualifiers**

Can not be in HLQ!

Profile Name: TSGLW.D%TAKEY.**

Dataset Names:

TSGLW.DATAKEY.NEW	YES
TSGLW.DETAKEY	YES
TSGLW.DATAKE	NO
TSGLW.DETAKEY.OLD	YES

Profile Name: TSGLW.R%%%.C*

Dataset Names:

TSGLW.RACF.CODE	YES
TSGLW.RACF2.CODE	NO
TSGLW.REXX.CODE.V2	NO
TSGLW.REXX.CODE	YES

Profile Name: TSG%%.JCL.** NO

Profile	Owner	UACC	Warning	Erase	Auditing	ACL	Segments
							....

```
ADDSD ‘TSGLW.JCL.C*’
UACC(NONE)
AUDIT(success(update) failures(read))
```

- The types of auditing required are:

ALL, FAILURES, SUCCESS, and NONE

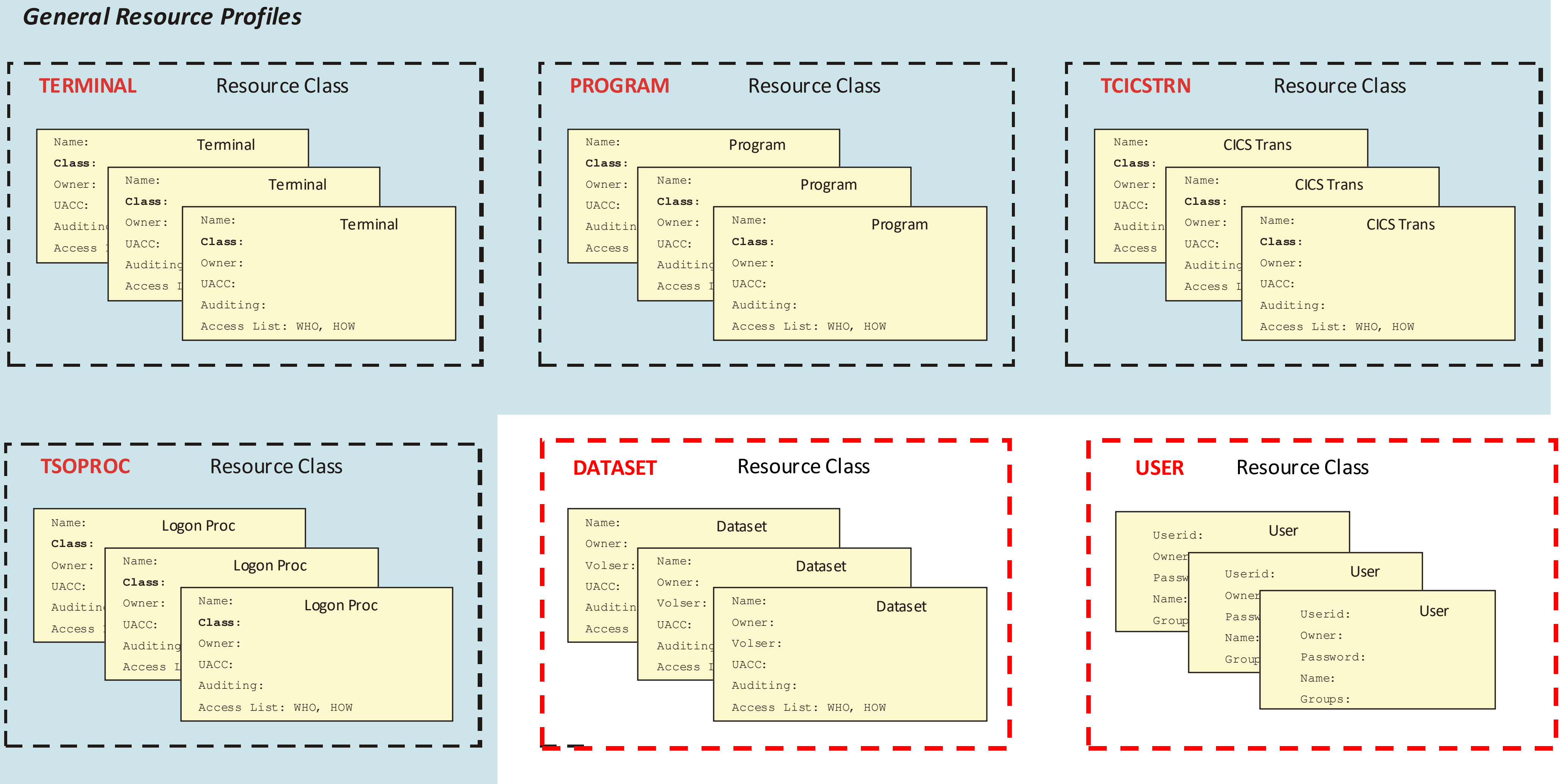
- Then the access level:
  - READ
  - UPDATE
  - CONTROL
  - ALTER

- The default, if AUDIT is not specified, is FAILURES(READ)

General Resource Profiles

VERTALI

Resource classes



General Resource Profiles

TERMINAL Resource Class

Name: Terminal
Class:
Owner:
UACC:
Auditing:
Access List: WHO, HOW

PROGRAM Resource Class

Name: Program
Class:
Owner:
UACC:
Auditing:
Access List: WHO, HOW

TCICSTRN Resource Class

Name: CICS Trans
Class:
Owner:
UACC:
Auditing:
Access List: WHO, HOW

TSOPROC Resource Class

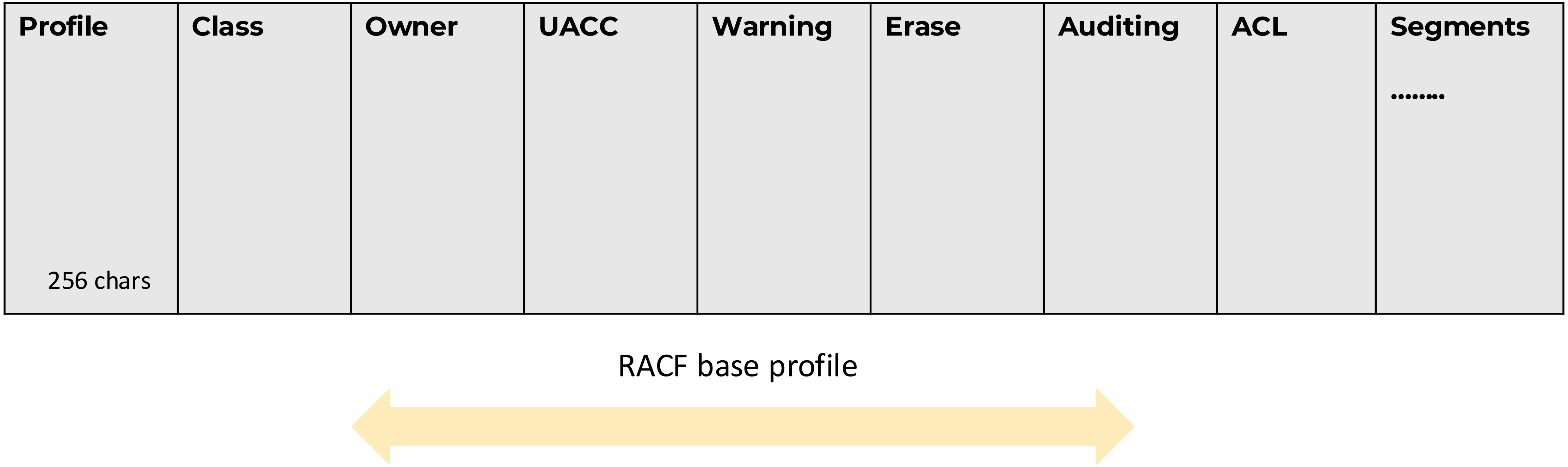
Name: Logon Proc
Class:
Owner:
UACC:
Auditing:
Access List: WHO, HOW

DATASET Resource Class

Name: Dataset
Owner:
Volser:
UACC:
Auditing:
Access List: WHO, HOW

USER Resource Class

Userid: User
Owner:
Password:
Name:
Groups:



Profile	Class	Owner	UACC	Warning	Erase	Auditing	ACL	Segments
256 chars								....

RACF base profile

General Resource Profiles

- Protect everything else!
- Both generic and discrete general resource profiles are allowed
- Wildcard characters can be used in any qualifier position
- Have to specify a CLASS
- Profiles are grouped by this CLASS
- Auditing attribute applies

Access Granted!
Access Denied!

User Profiles

Group Profiles

User Profiles

Dataset Profiles

Resource Profiles

Dataset Profiles

TSGLW.JCL.**

Avengers	READ
Thor	UPDATE
Loki	ALTER

Resource Profiles

Class UNIXPRIV
SUPERUSER.FILESYS.CHOWN

Avengers	ALTER
Thor	UPDATE
Loki	READ

Access permissions are specified in three ways:

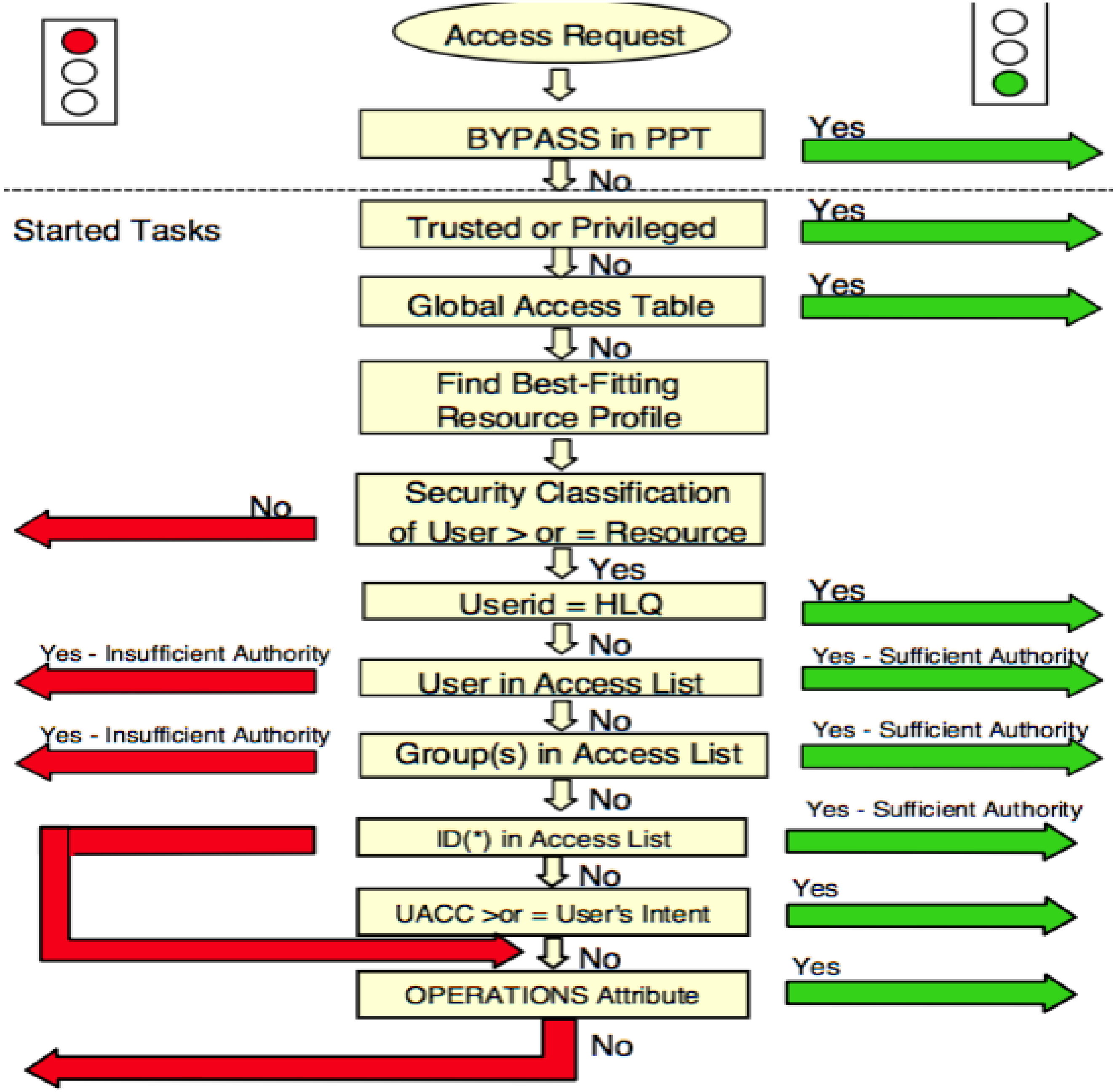
– Standard Access List

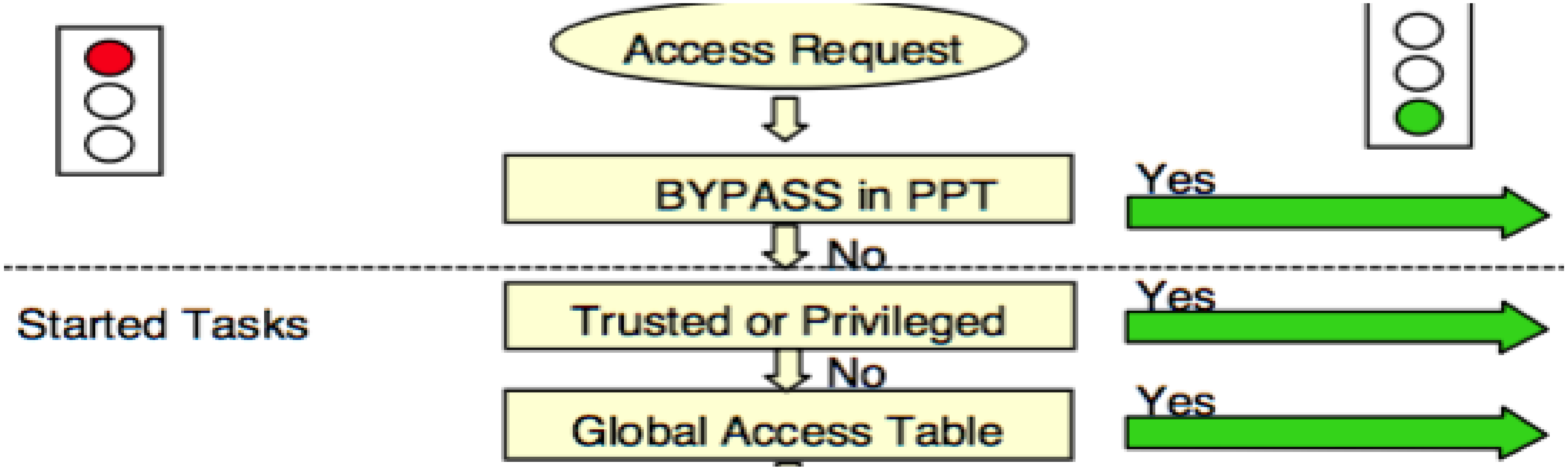
– Conditional Access List

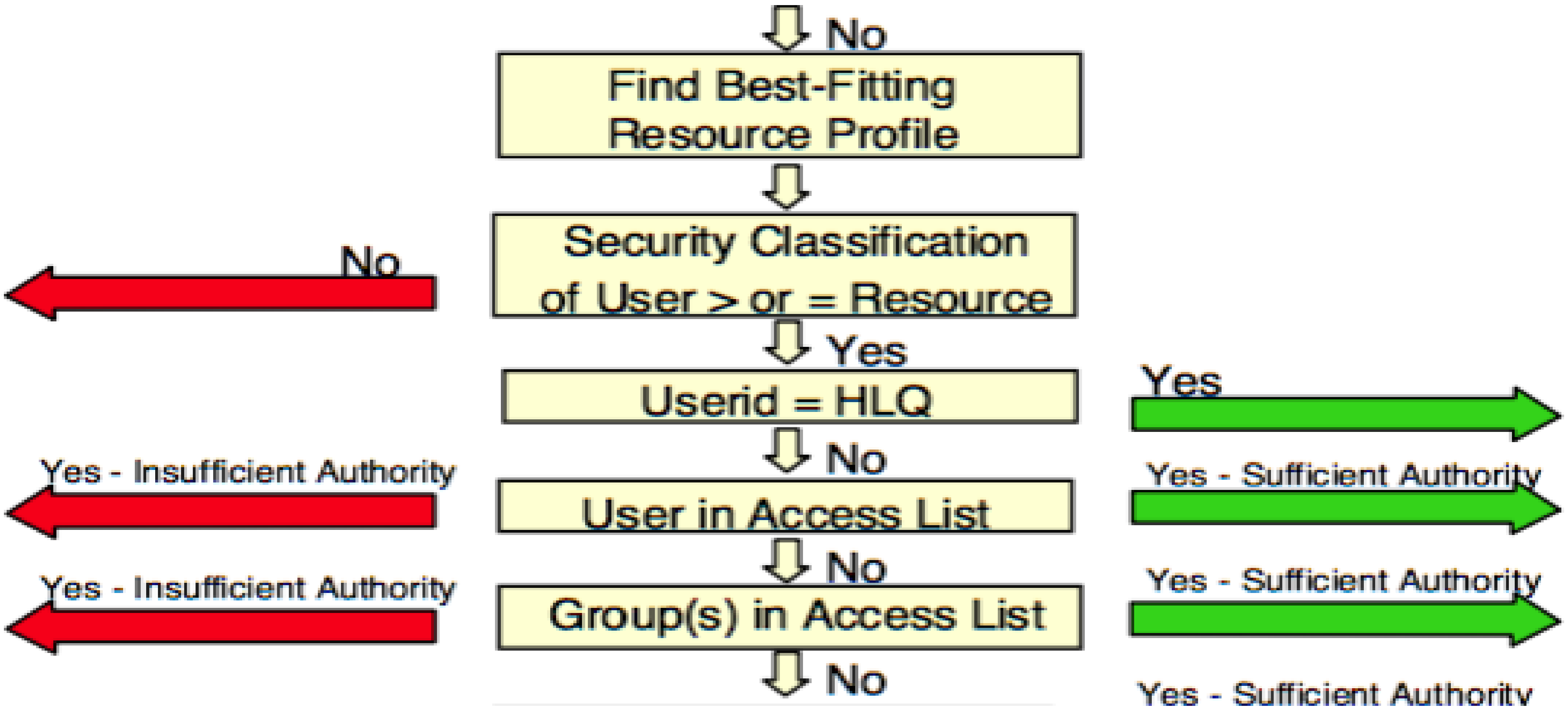
– Universal Access (UACC) - default access granted to anyone

Access can be permitted to:

- – USERID
- – Group
- – ID(*) - Grants access to all RACF- defined users
- – Granted by attribute OPERATIONS


Access Request
BYPASS in PPT
Yes
No
Started Tasks
Trusted or Privileged
Yes
No
Global Access Table
Yes
No
Find Best-Fitting Resource Profile
Security Classification of User > or = Resource
No
Yes
Userid = HLQ
Yes
No
Yes - Insufficient Authority
User in Access List
Yes - Sufficient Authority
No
Yes - Insufficient Authority
Group(s) in Access List
Yes - Sufficient Authority
No
Yes - Sufficient Authority
ID(*) in Access List
No
UACC >or = User's Intent
Yes
No
OPERATIONS Attribute
Yes
No


Access Request
BYPASS in PPT
Yes
No
Started Tasks
Trusted or Privileged
Yes
No
Global Access Table
Yes



No

Find Best-Fitting Resource Profile

Security Classification of User > or = Resource

No

Yes

Userid = HLQ

Yes

No

User in Access List

Yes - Insufficient Authority

Yes - Sufficient Authority

No

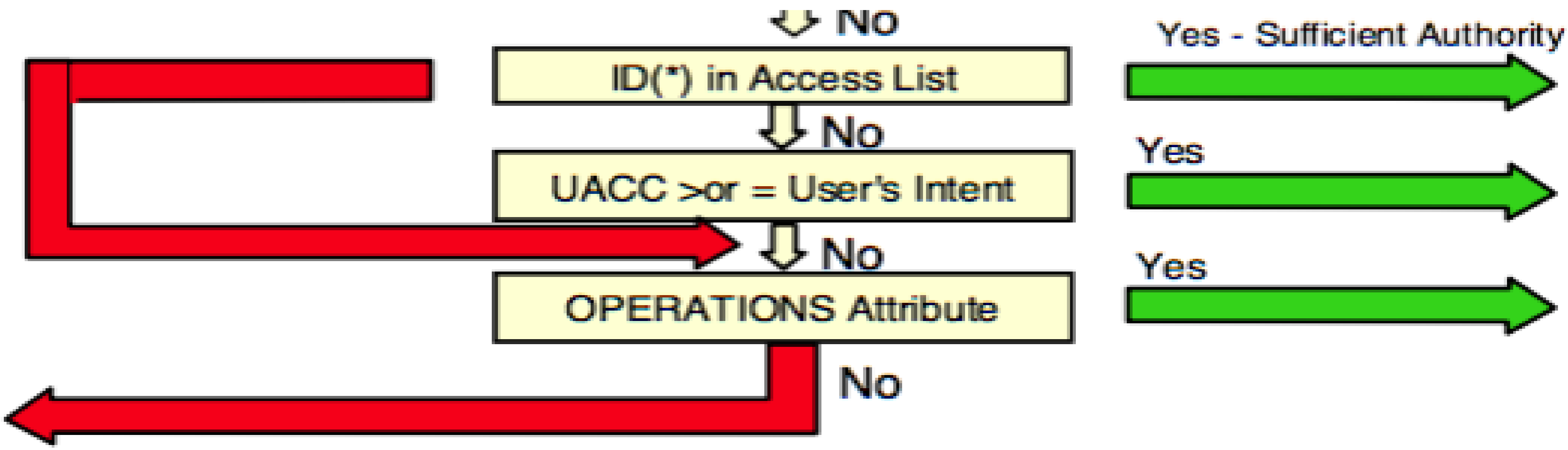
Group(s) in Access List

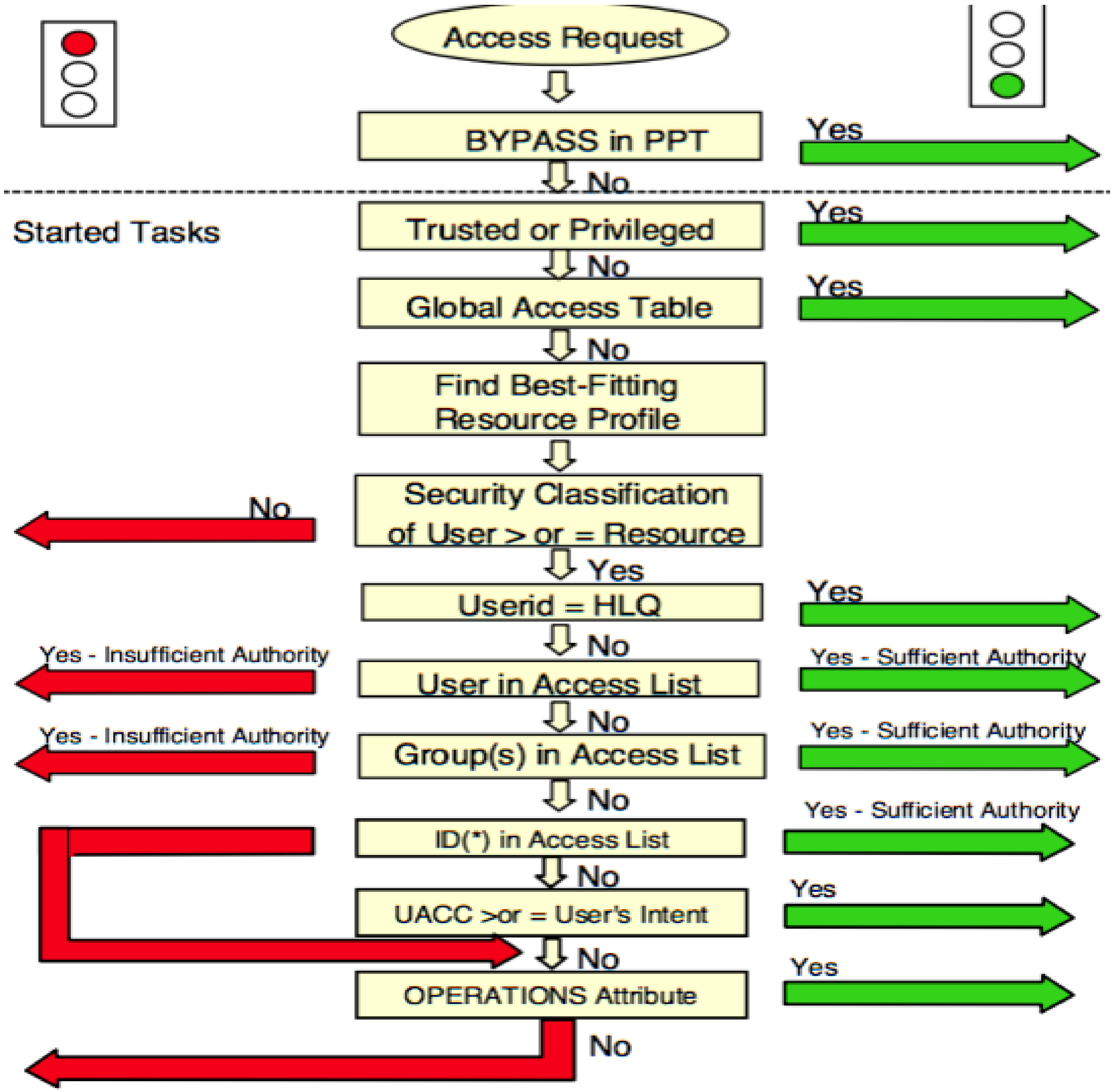
Yes - Insufficient Authority

Yes - Sufficient Authority

No

Yes - Sufficient Authoritv


No
ID(*) in Access List
Yes - Sufficient Authority
No
UACC >or = User's Intent
Yes
No
OPERATIONS Attribute
Yes
No



Access Request

BYPASS in PPT — Yes / No

Started Tasks

Trusted or Privileged — Yes / No

Global Access Table — Yes / No

Find Best-Fitting Resource Profile

Security Classification of User > or = Resource — No / Yes

Userid = HLQ — Yes / No

User in Access List — Yes - Insufficient Authority / Yes - Sufficient Authority / No

Group(s) in Access List — Yes - Insufficient Authority / Yes - Sufficient Authority / No

ID(*) in Access List — Yes - Sufficient Authority / No

UACC >or = User's Intent — Yes / No

OPERATIONS Attribute — Yes / No

Summary

- The bigger picture – subsystem & application configuration, SETROPTS, auditing, SMF configuration, exits
- A profile is just a list of protection parameters for a specific resource, and a list of users who can access the resource
- Resources are grouped together by class
- Be mindful of privileged user attributes

THANK YOU

VERTALI