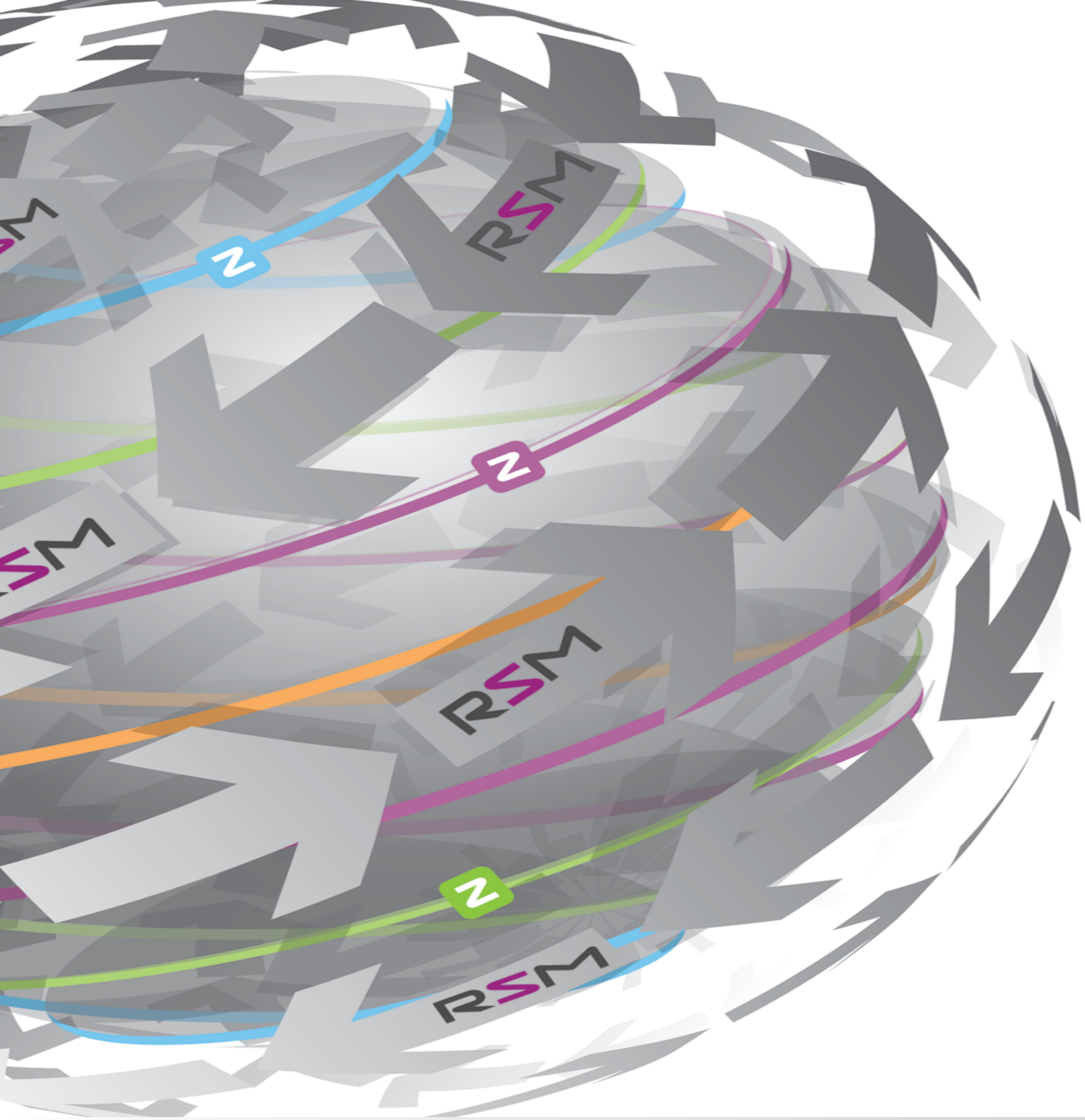


RSM PARTNERS

World Class z Specialists

RACF For Dummies

Presented by a Dummy

Leanne Wilson

Introduction

- Leanne Wilson
- Security consultant
- Worked at RSM Partners for 7 years
- Worked on a number of security based pr

AGENDA

RACF Overview

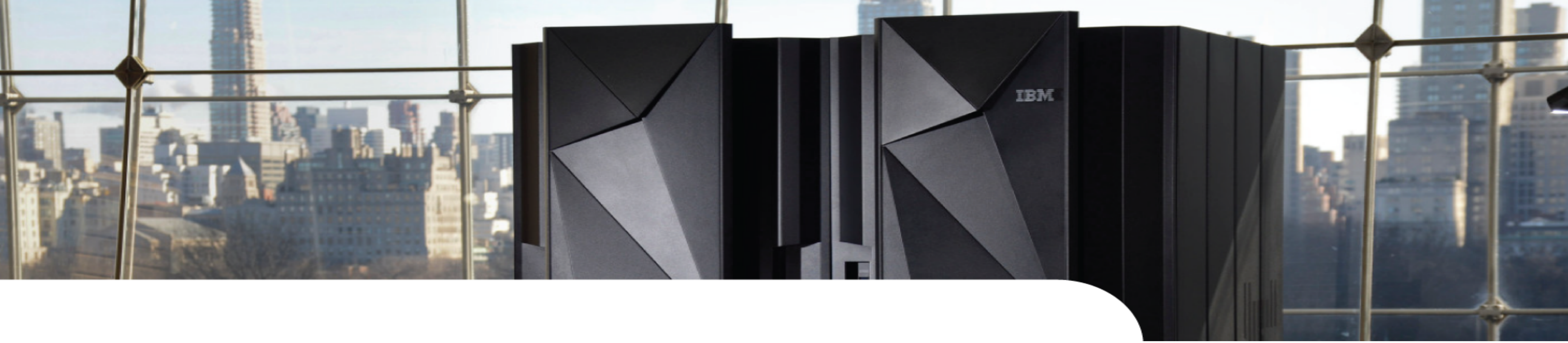
User & Group Profiles

Dataset & General Resource Profiles

Access Granted! Access Denied!

Auditing & Utilities

Summary



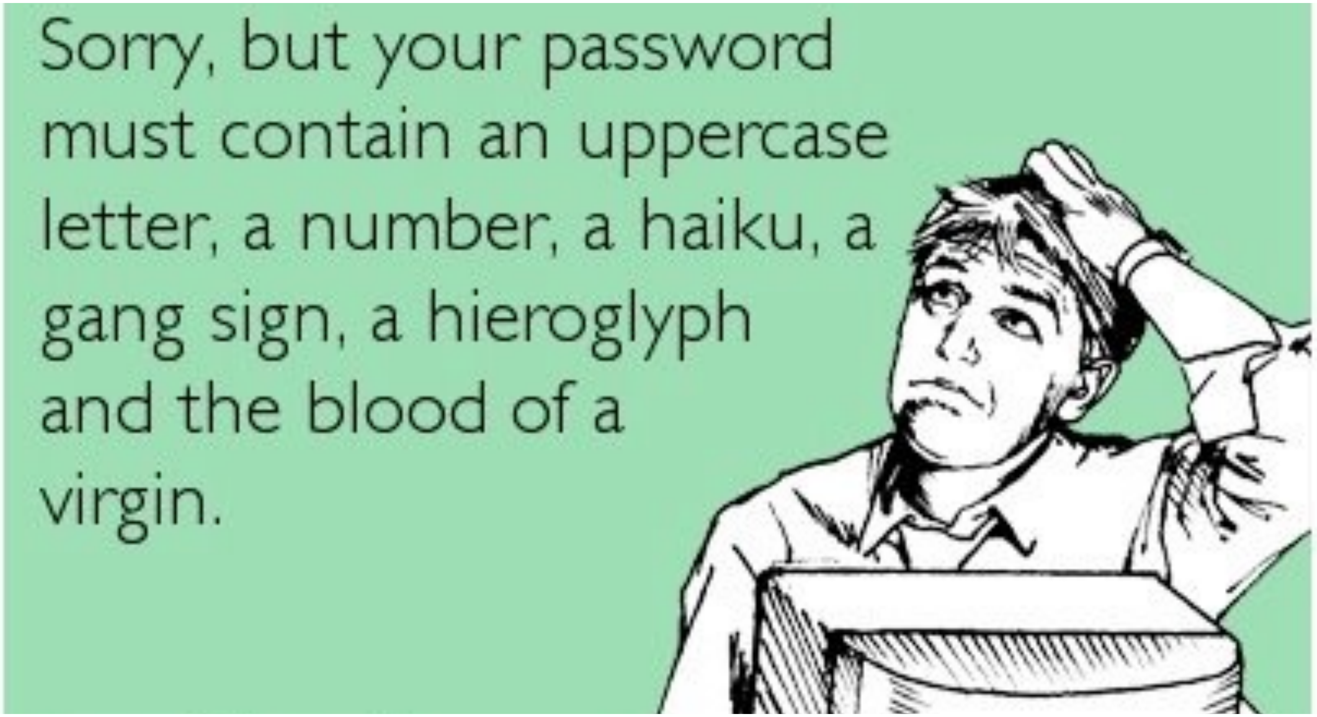
Overview

What is security?

The protection of data from unauthorised*:*

- Destruction
- Modification
- Disclosure
- Use

Whether accidental or intentional!

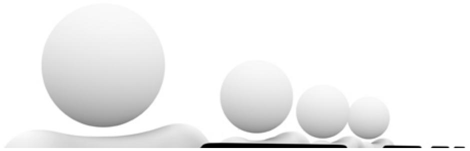


Sorry, but your password must contain an uppercase letter, a number, a haiku, a gang sign, a hieroglyph and the blood of a virgin.

What security do we need?

Protect the data & resources

Control the users



Isolate the network

What is RACF?

R ESOURCE

A ACCESS

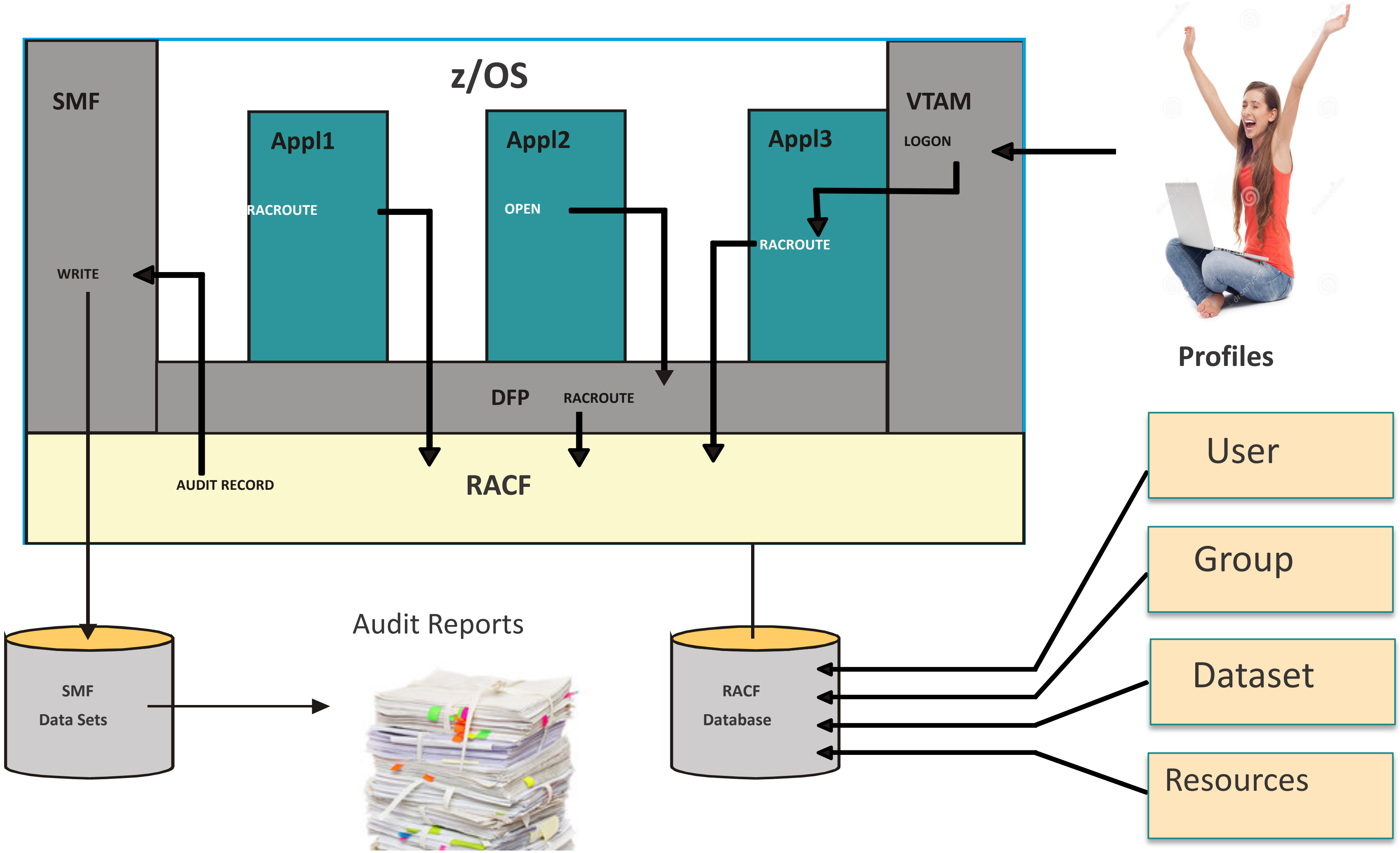
C ONTROL

F ACILITY

What is RACF? Resource Access Control Facility

- 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



How Can RACF Help?

User Profiles

Group Profiles

User Profiles

Dataset Profiles

Resource Profiles

Example ACL

Dataset Profiles

Resource Profiles

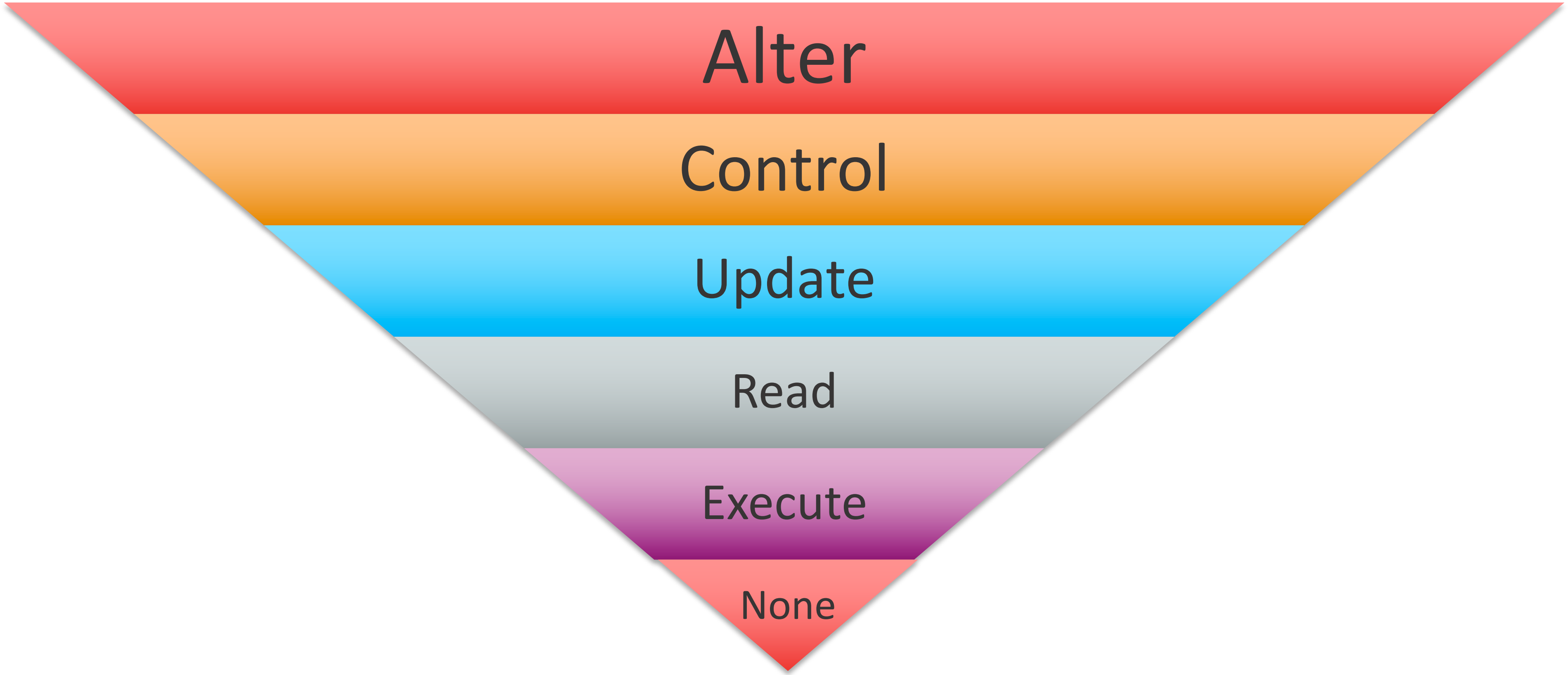
TSGLW.JCL.**

Avengers	READ
Thor	UPDATE
Loki	ALTER

Class UNIXPRIV
SUPERUSER.FILESYS.CHOWN

Avengers	ALTER
Thor	UPDATE
Loki	READ

Access levels



Alter

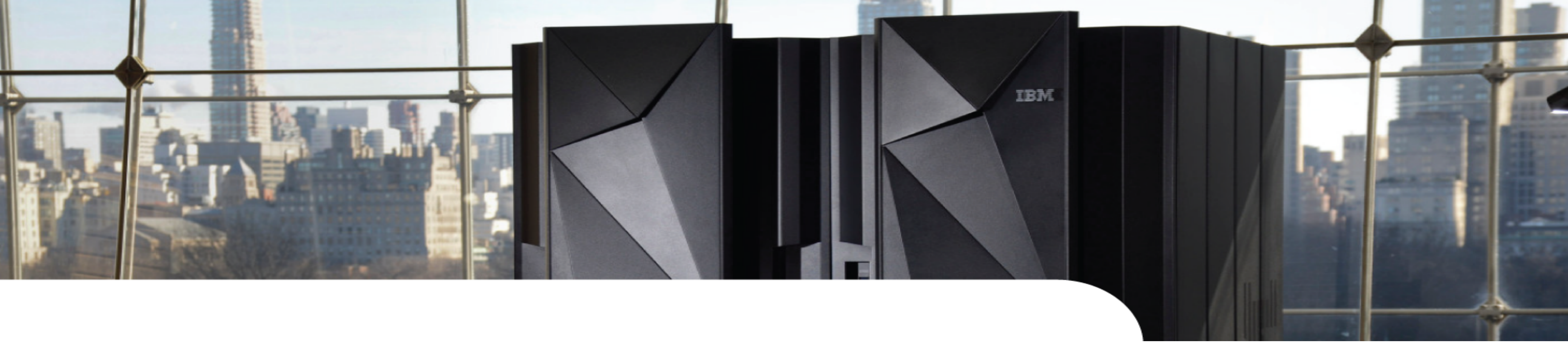
Control

Update

Read

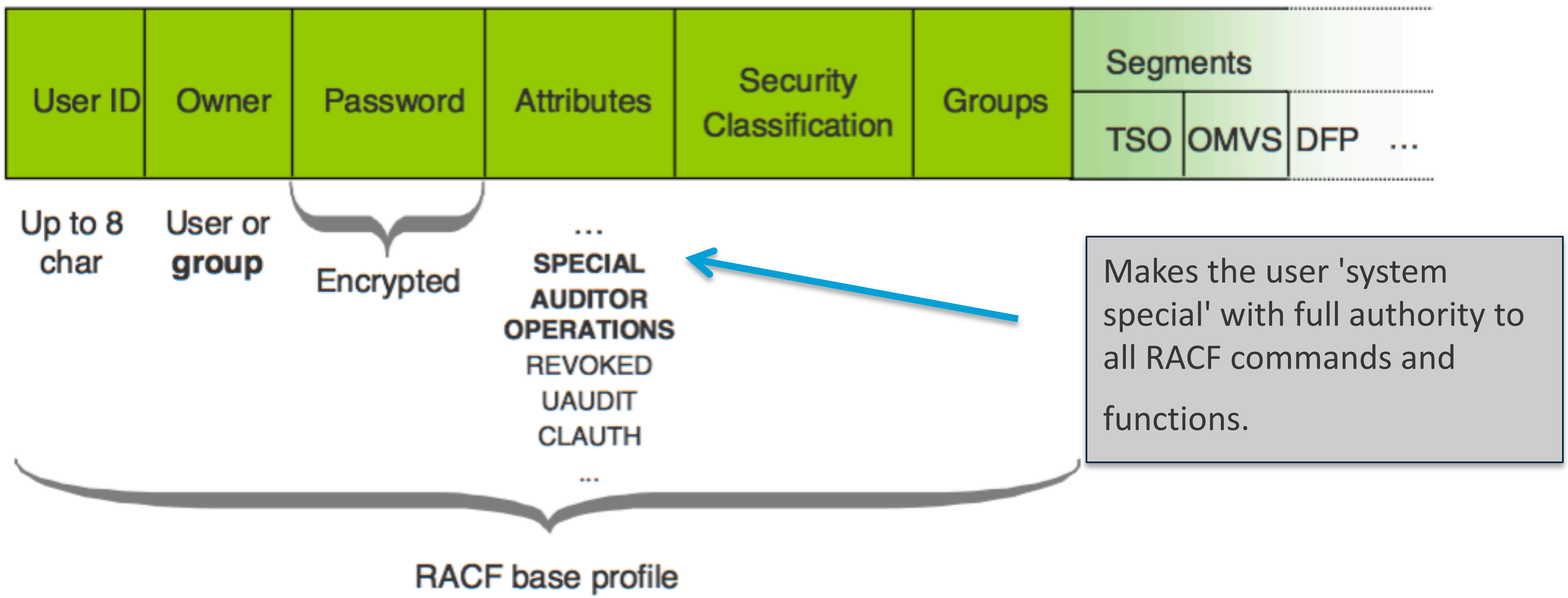
Execute

None



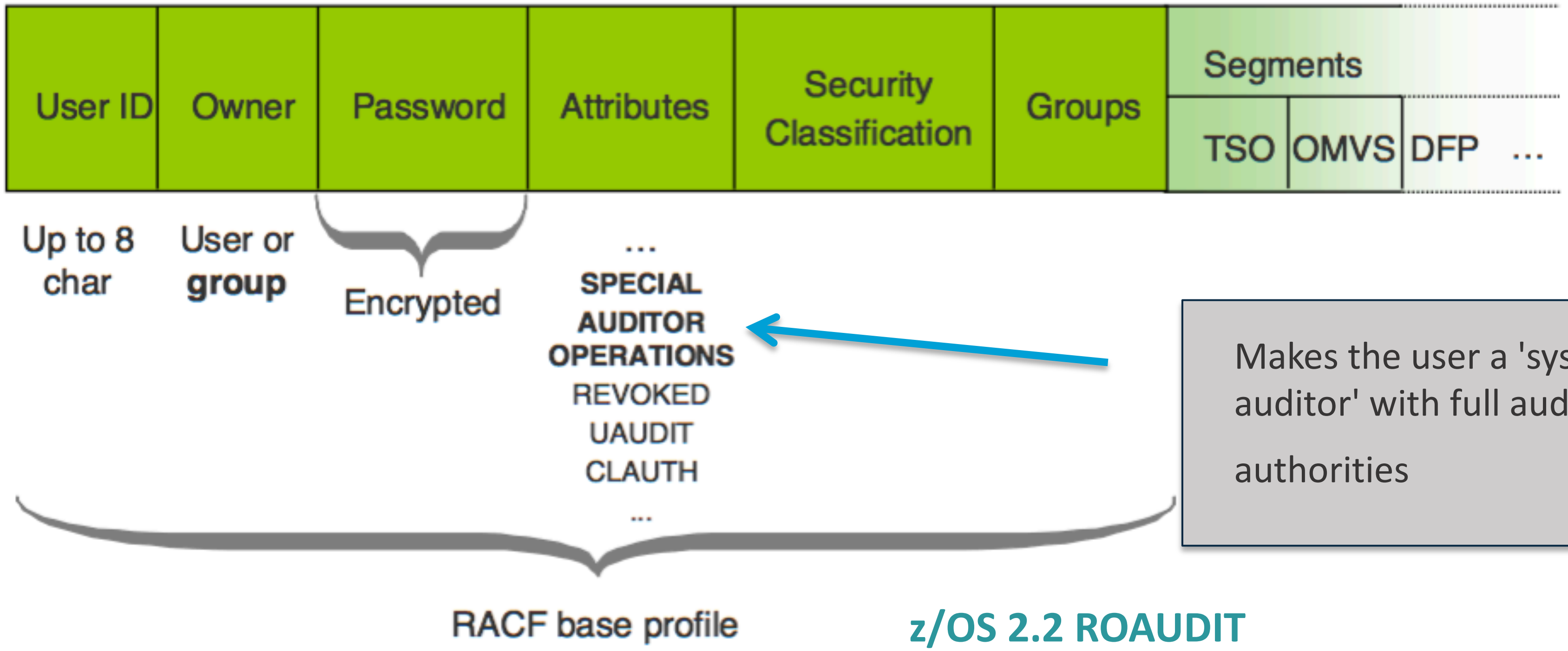
User Profiles

User Profile



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

User Profile



User ID | Owner | Password | Attributes | Security Classification | Groups | Segments: TSO, OMVS, DFP ...

Up to 8 char

User or **group**

Encrypted

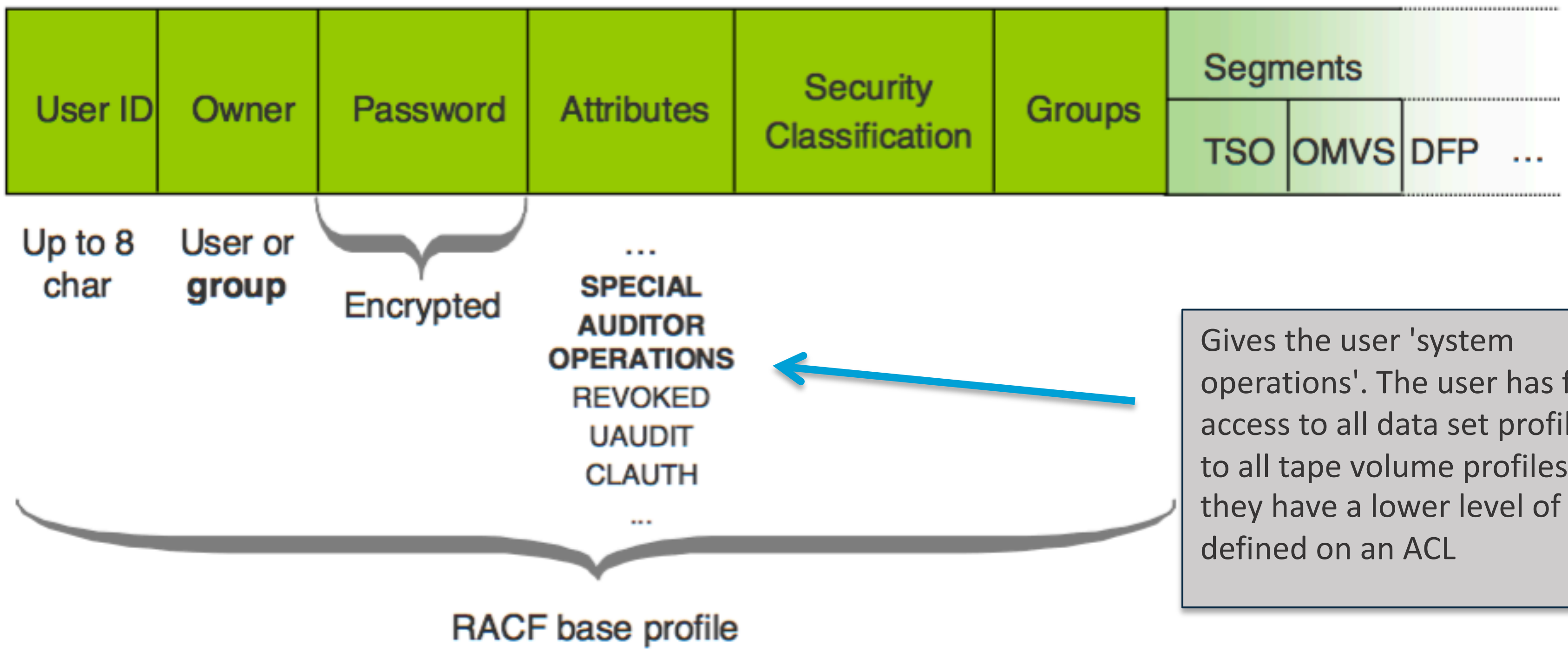
...
SPECIAL
AUDITOR
OPERATIONS
REVOKED
UAUDIT
CLAUTH
...

RACF base profile

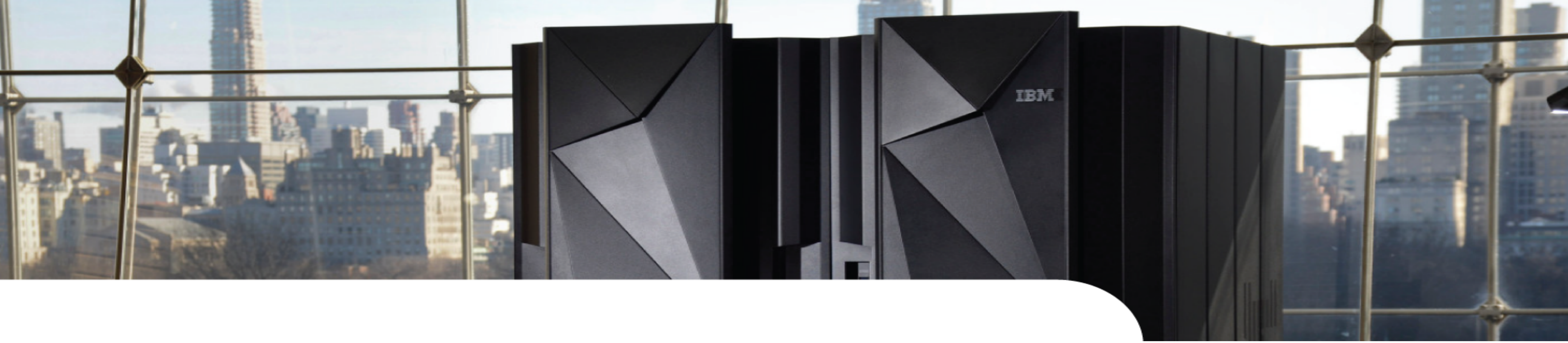
Makes the user a 'system auditor' with full auditing authorities

z/OS 2.2 ROAUDIT

User Profile

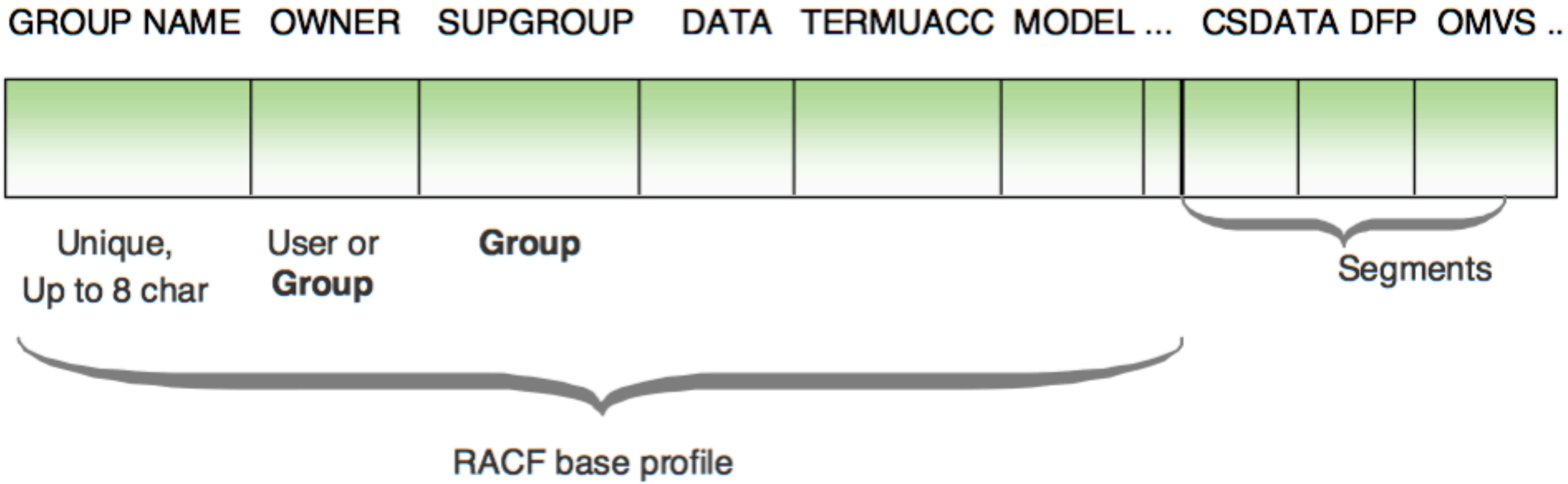


Gives the user 'system operations'. The user has full access to all data set profiles and to all tape volume profiles. Unless they have a lower level of access defined on an ACL



Group Profiles

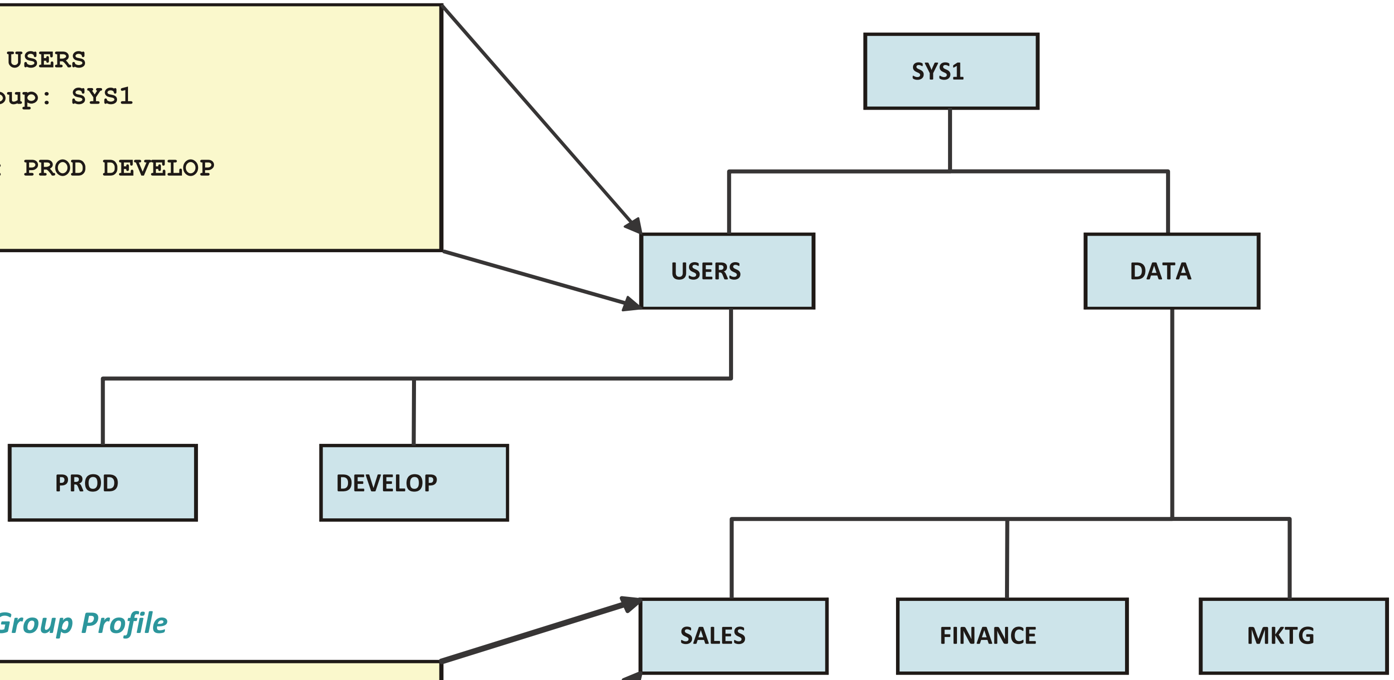
Group Profile



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

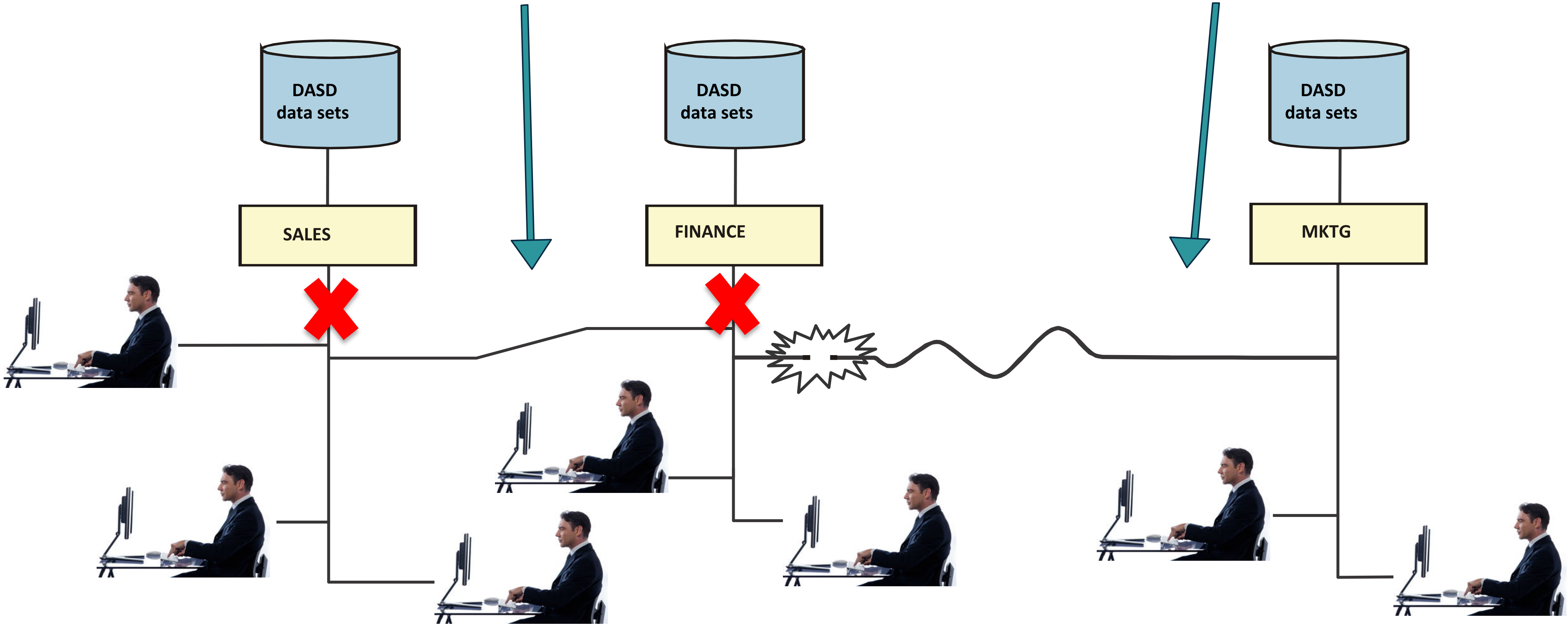
Belong to the same department

Do the same job

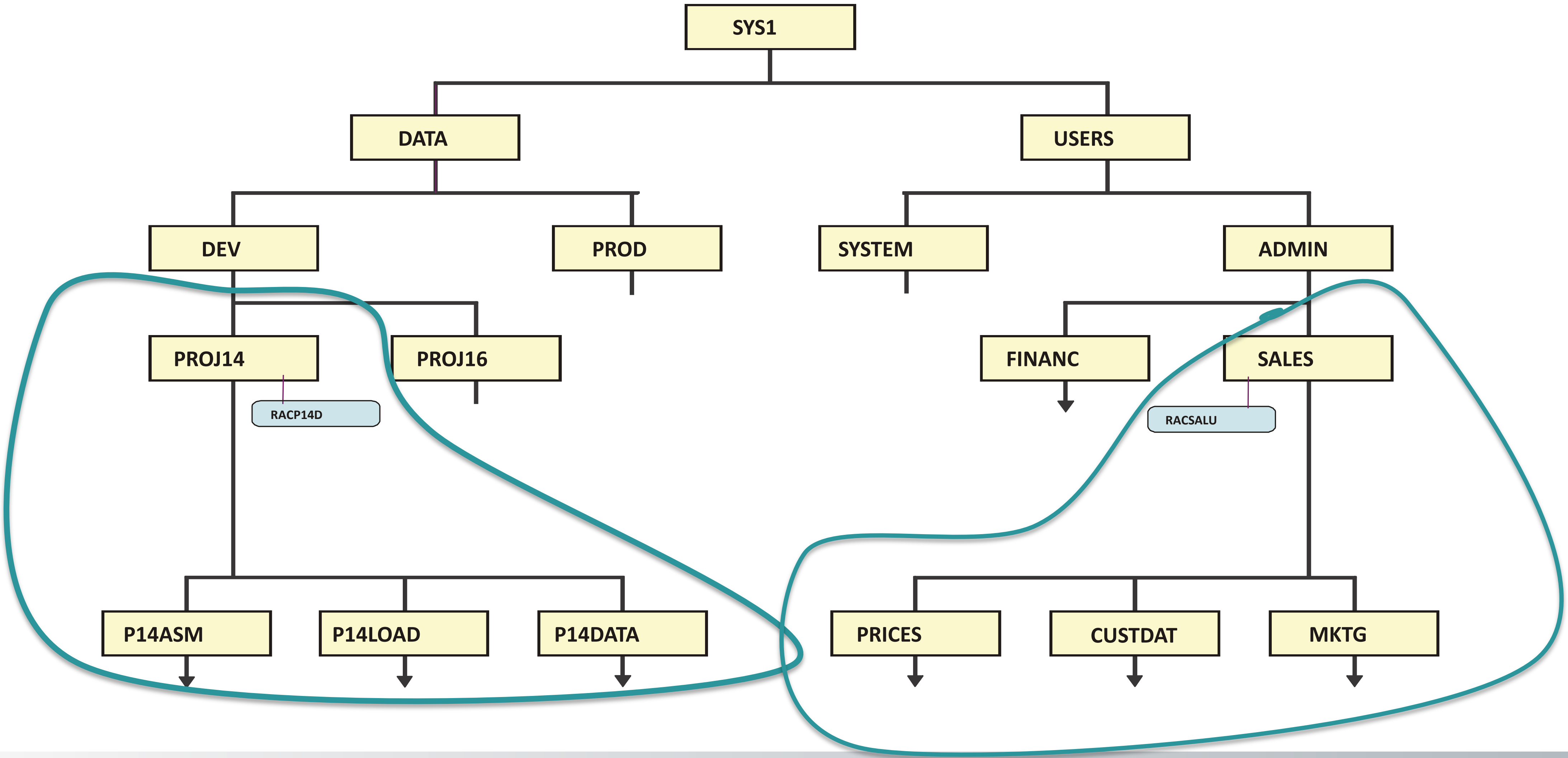
Users and groups

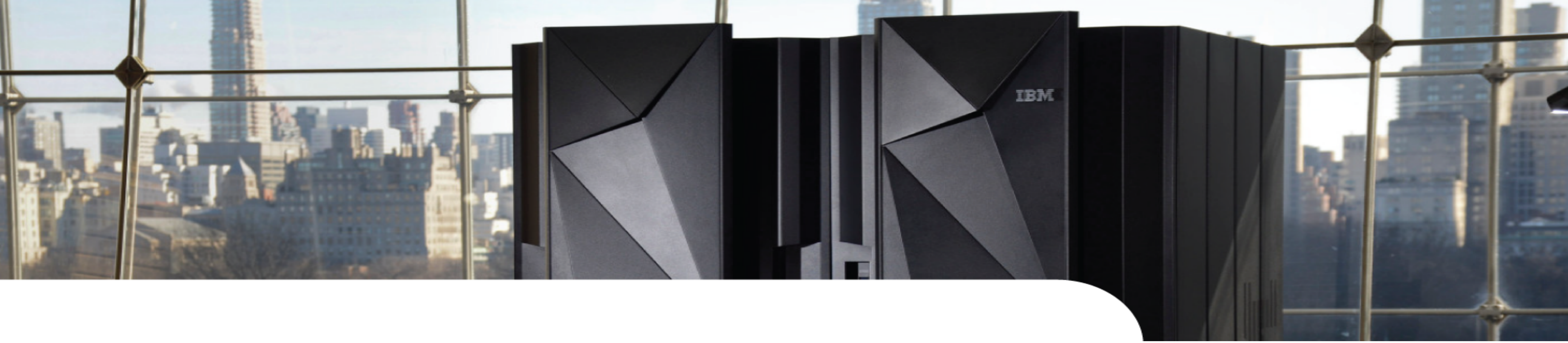
Users who are connected to multiple groups, get access to all resources to which the groups have access

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



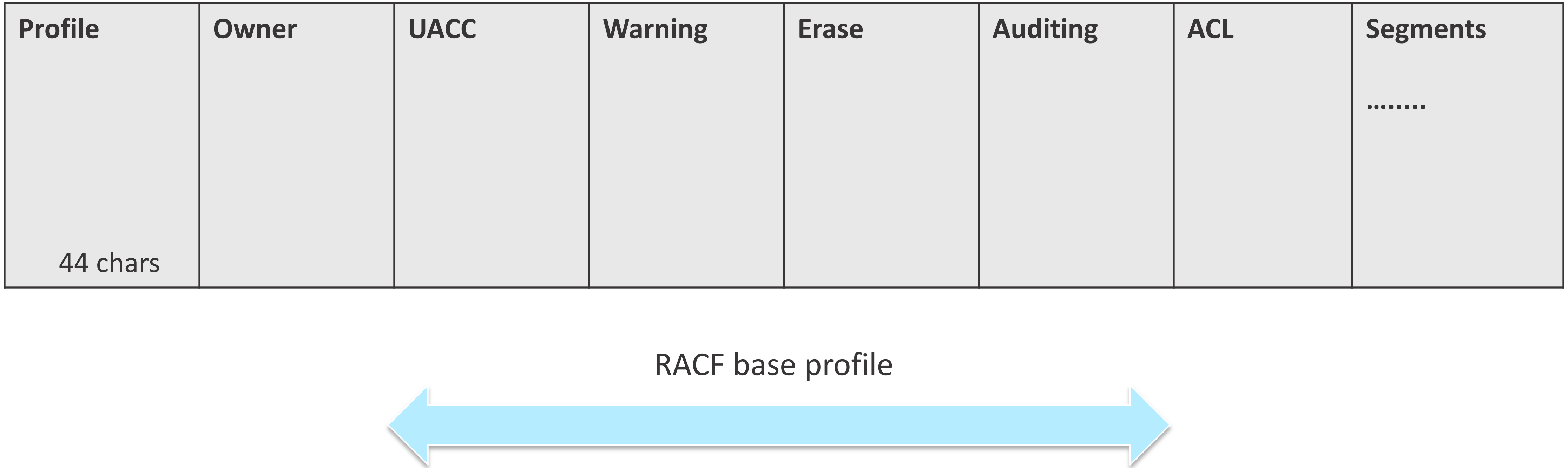
Group Level Attributes





Dataset Profiles

Dataset Profile



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

How to Protect Resources

Generic Profiles

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

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

Discrete Profiles

- TSGLW.JCL.CNTL

All examples are listed as if EGN is activated

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**

<u>**Can not be in HLQ!**</u>

Generic Wildcard Characters

Profile Name: TSGLW.D%TAKEY.**

Dataset Names:	TSGLW.DATAKEY.NEW	YES
	TSGLW.DETAKEY	YES
	TSGLW.DATAKE	NO
	TSGLW.DETAKEY.OLD	YES

Generic Wildcard Characters

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

Auditing Attributes

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

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

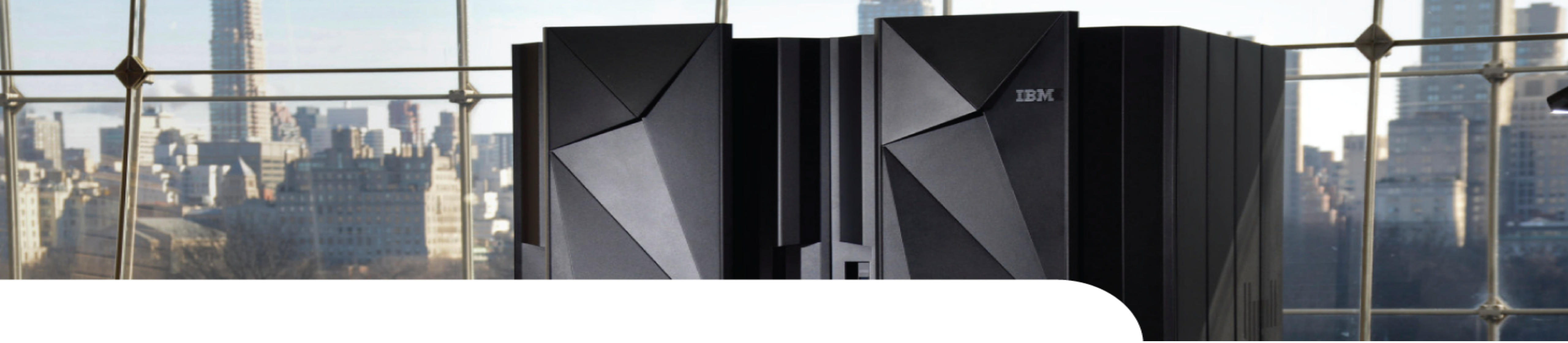
Auditing Attributes

- The types of auditing required are:

ALL, FAILURES, SUCCESS, and NONE

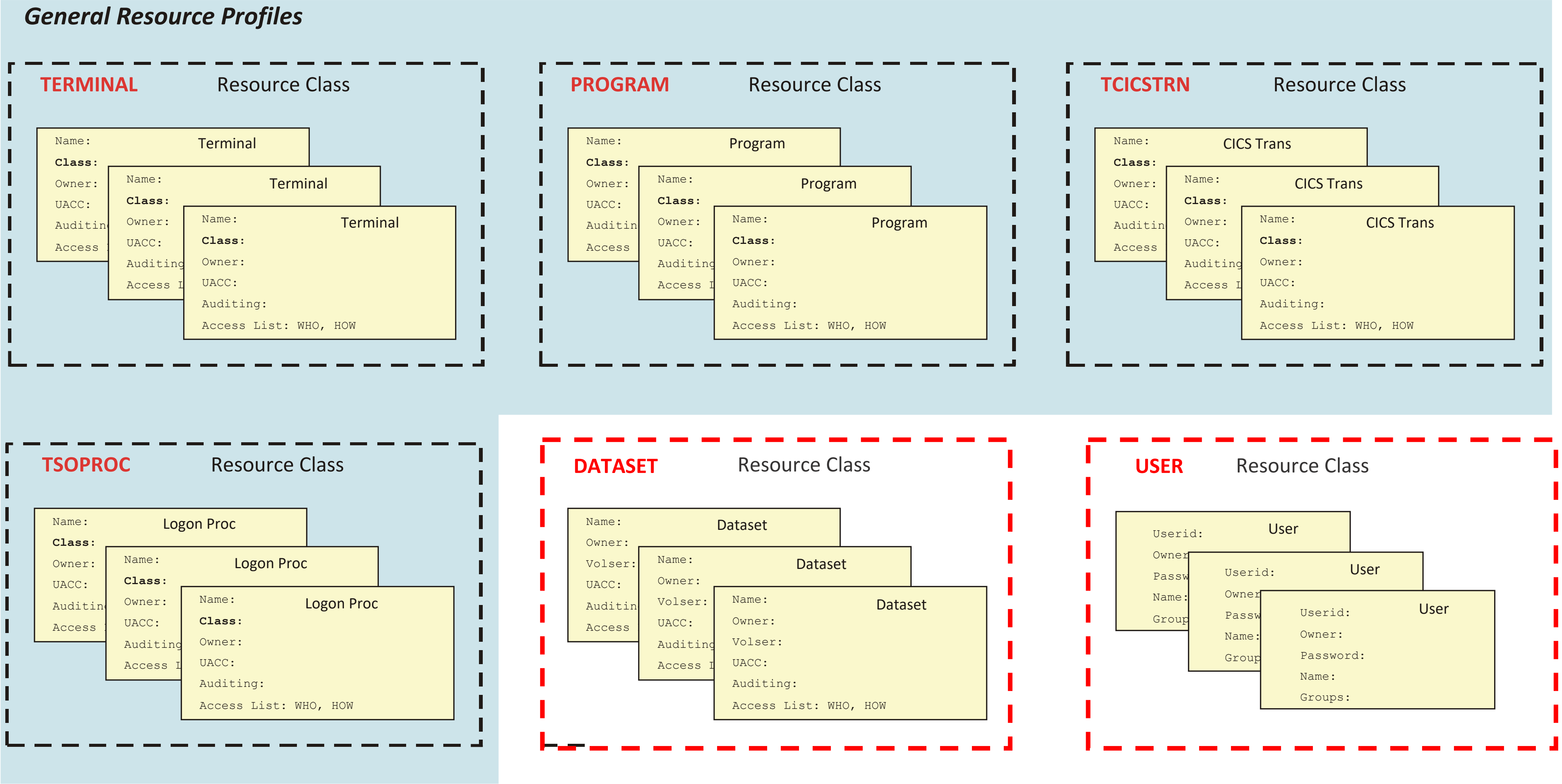
- Then the access level:
  - READ
  - UPDATE
  - CONTROL
  - ALTER

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



General Resource Profiles

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:

General Resource Profile

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!

Example ACL

User Profiles

Group Profiles

User Profiles

Dataset Profiles

Resource Profiles

Example ACL

Dataset Profiles

Resource Profiles

TSGLW.JCL.**

Avengers	READ
Thor	UPDATE
Loki	ALTER

Class UNIXPRIV
SUPERUSER.FILESYS.CHOWN

Avengers	ALTER
Thor	UPDATE
Loki	READ

Access lists

- Conditional access lists have additional restrictions on the access

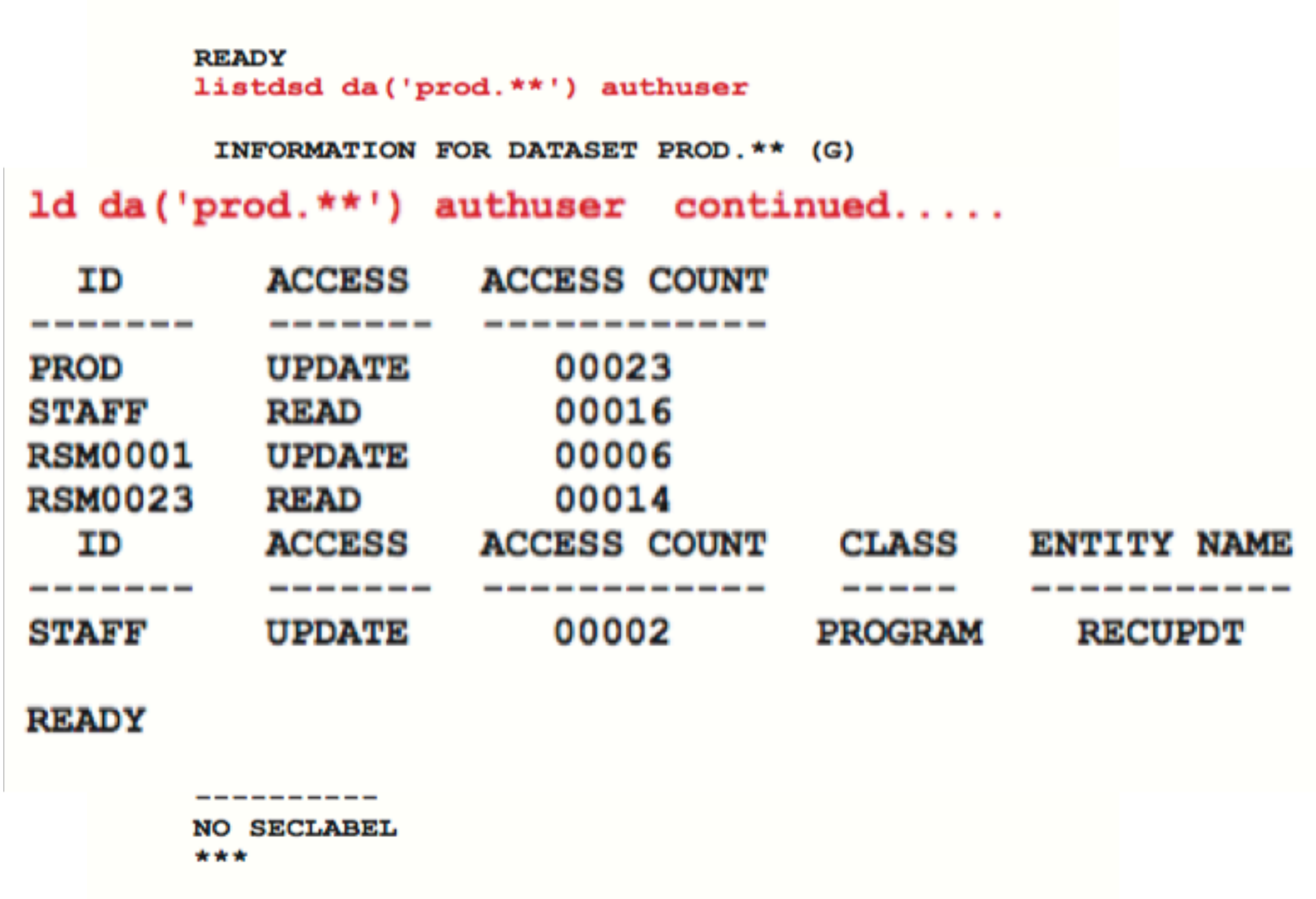
- For example: You can require that

  - a user be logged onto a particular terminal
  - when executing a particular program

Access lists

- 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



```
READY
listdsd da('prod.**') authuser

 INFORMATION FOR DATASET PROD.** (G)
```

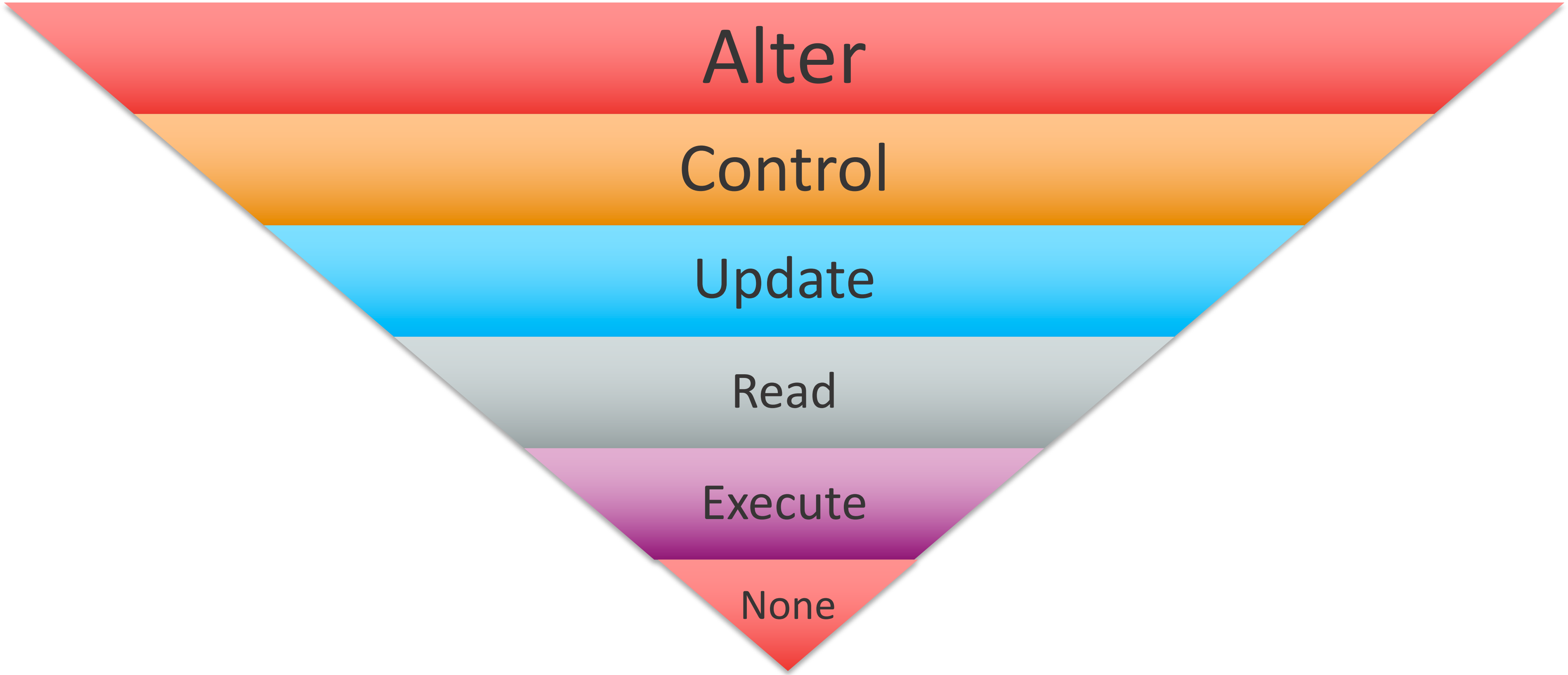
```
ld da('prod.**') authuser  continued.....

  ID        ACCESS    ACCESS COUNT
--------   --------   ------------
PROD        UPDATE       00023
STAFF       READ         00016
RSM0001     UPDATE       00006
RSM0023     READ         00014
  ID        ACCESS    ACCESS COUNT    CLASS    ENTITY NAME
--------   --------   ------------    ------   -----------
STAFF       UPDATE       00002       PROGRAM     RECUPDT

READY
```

```
----------
NO SECLABEL
***
```

Access levels



Alter

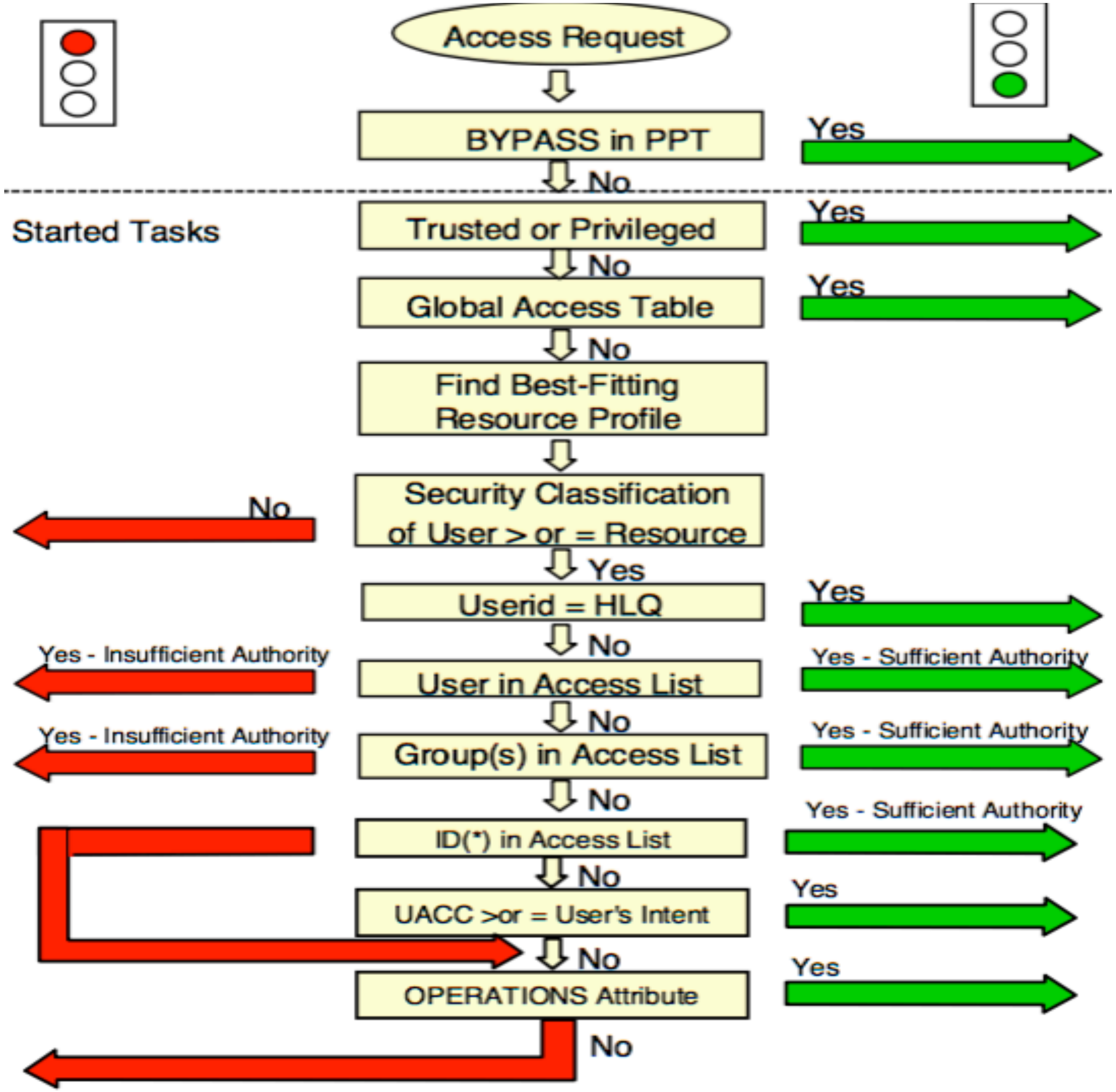
Control

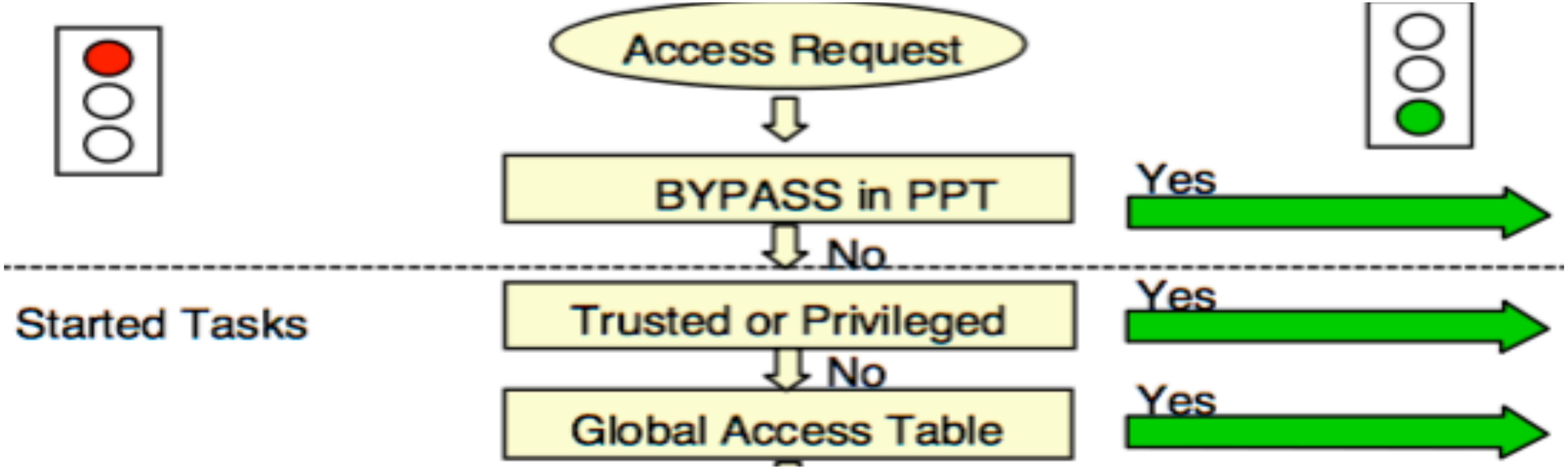
Update

Read

Execute

None


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

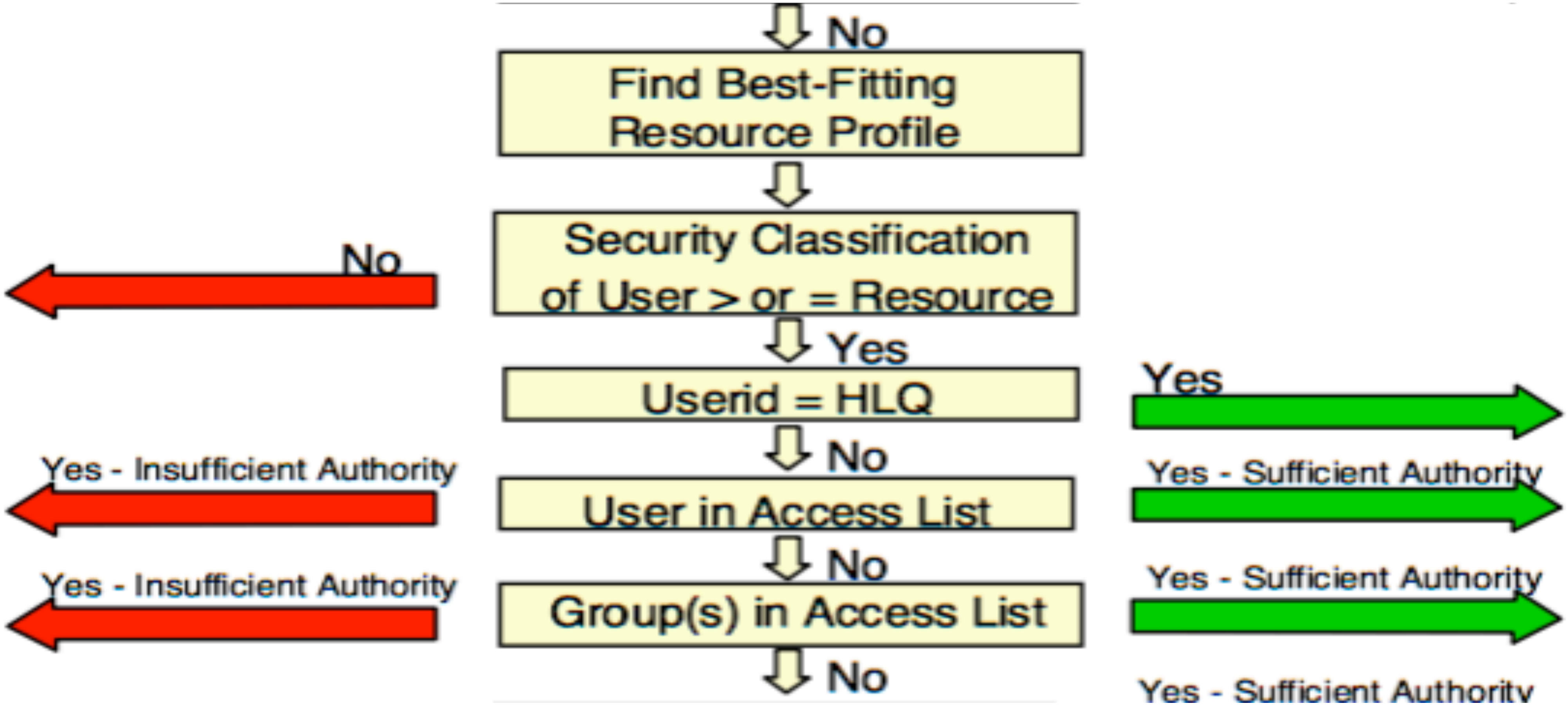
Trusted or Privileged

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

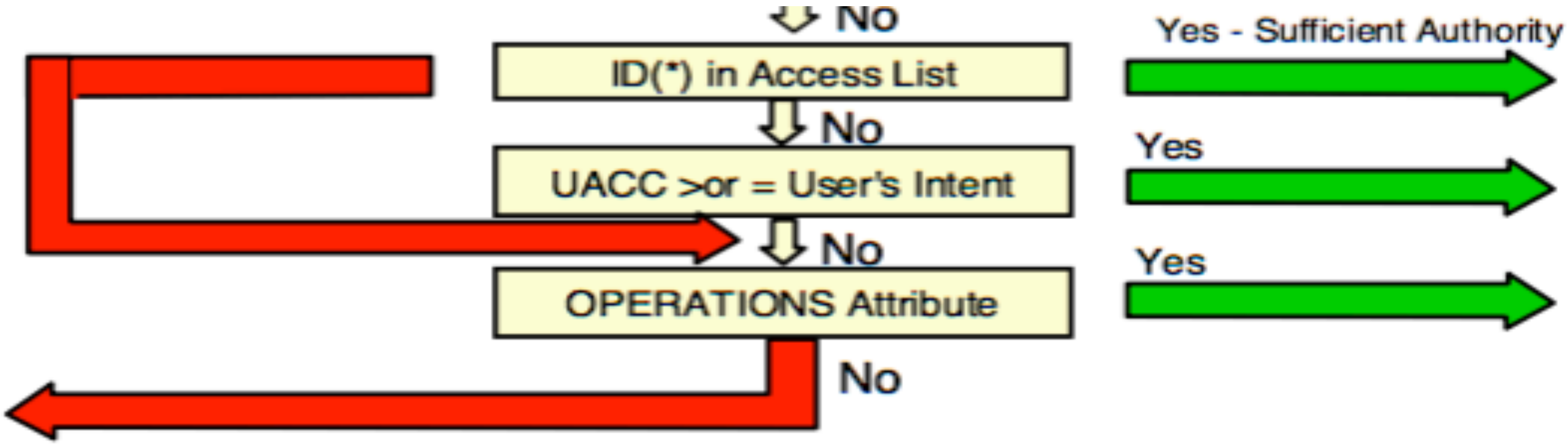
Group(s) in Access List

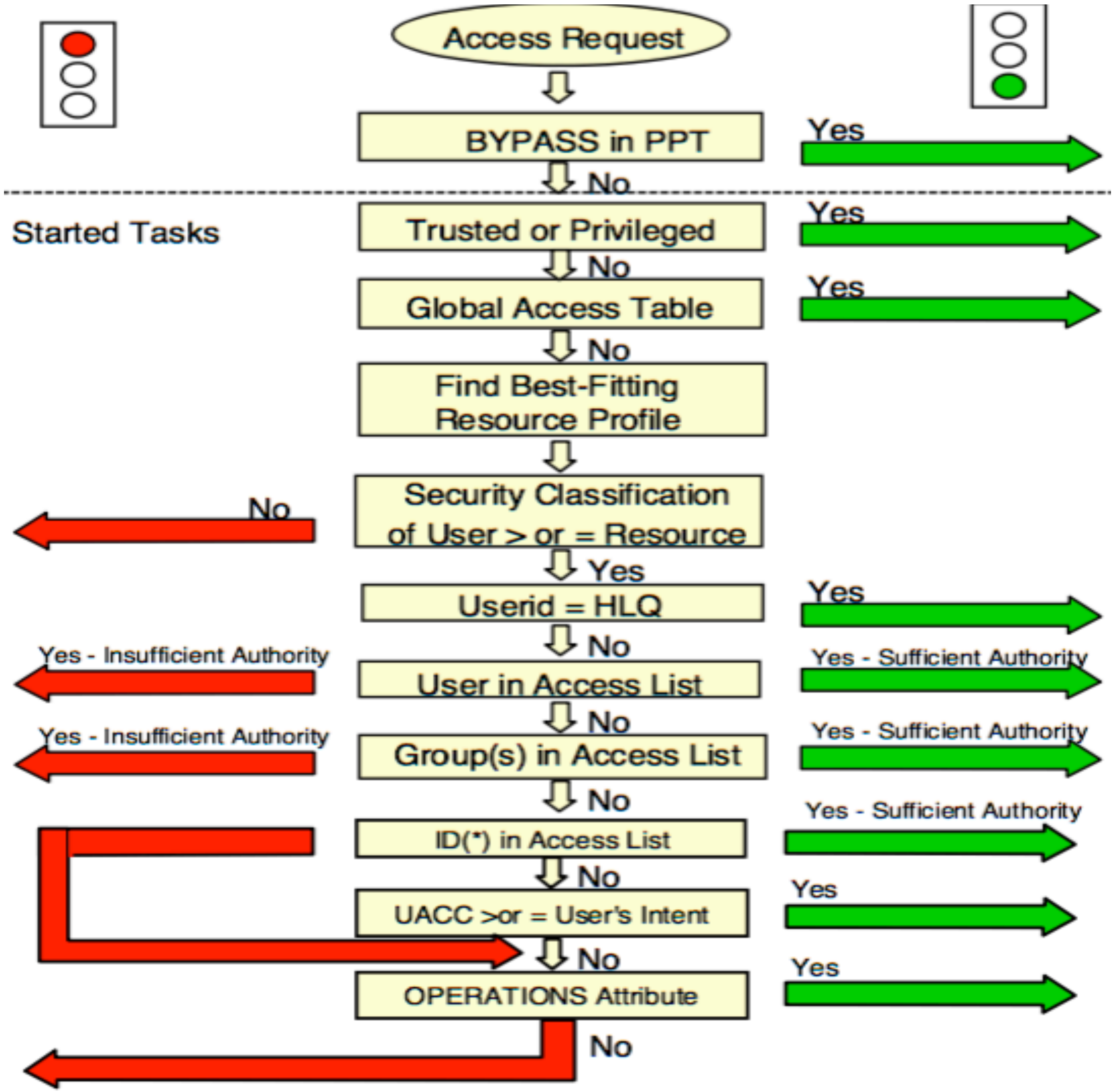
Yes - Insufficient Authority

Yes - Sufficient Authority

No

Yes - Sufficient Authority

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

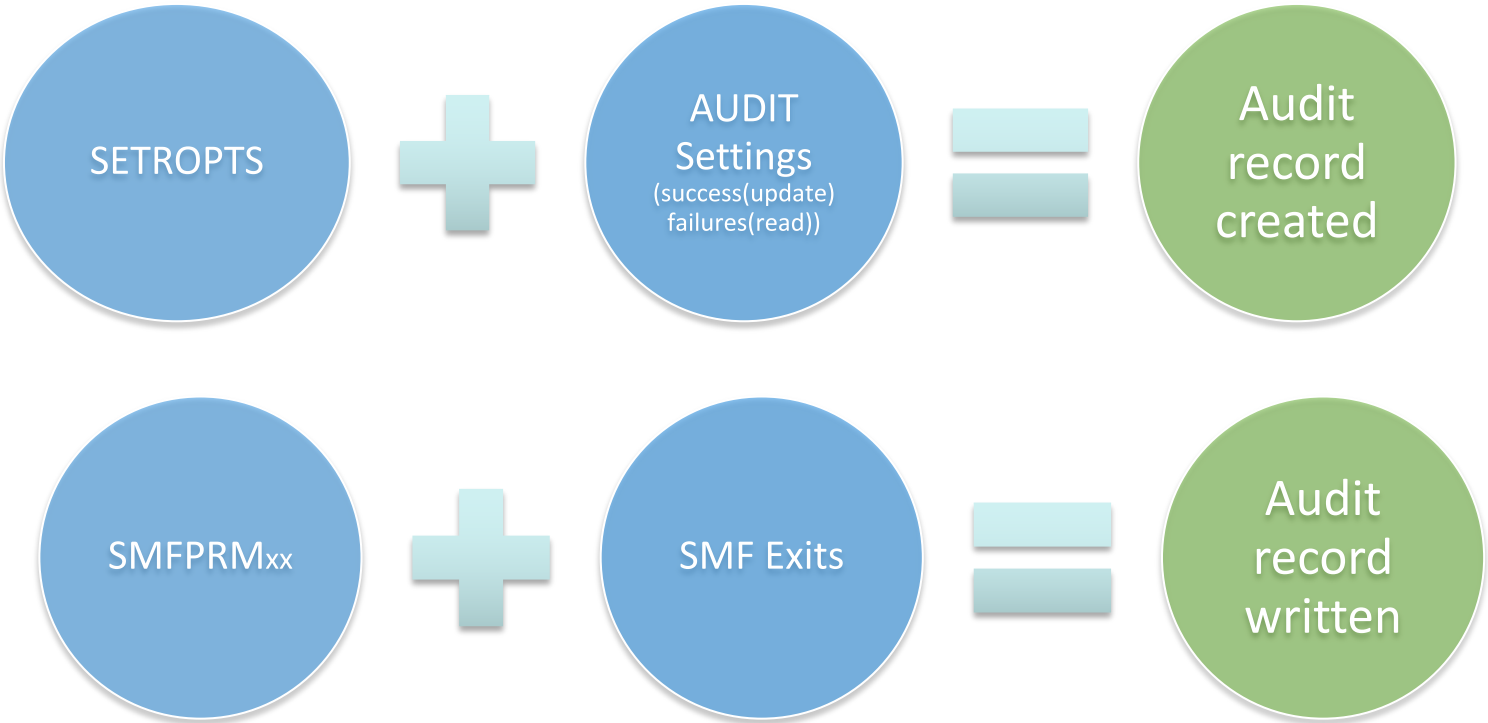
No

OPERATIONS Attribute — Yes

No

Auditing

Auditing


SETROPTS
AUDIT Settings (success(update) failures(read))
Audit record created
SMFPRMxx
SMF Exits
Audit record written

SETROPTS

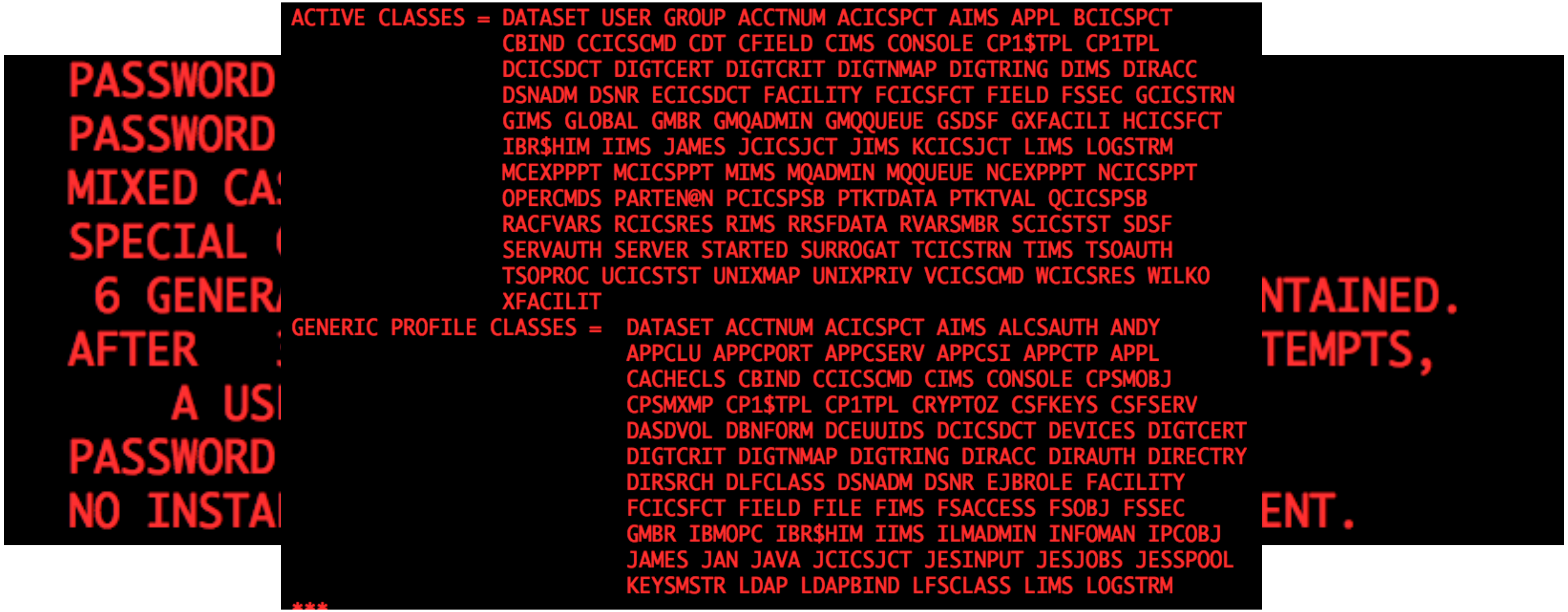
- SET RACF OPTIONS

- Defines system-wide RACF security & auditing options via SETROPTS commands or appropriate panels

- SPECIAL - List & set security options only
- AUDITOR - List all options & set auditing options
- ROAUDITOR - List all options

New in z/OS 2.2

SETROPTS



```
ACTIVE CLASSES = DATASET USER GROUP ACCTNUM ACICSPCT AIMS APPL BCICSPCT
                 CBIND CCICSCMD CDT CFIELD CIMS CONSOLE CP1$TPL CP1TPL
                 DCICSDCT DIGTCERT DIGTCRIT DIGTNMAP DIGTRING DIMS DIRACC
                 DSNADM DSNR ECICSDCT FACILITY FCICSFCT FIELD FSSEC GCICSTRN
                 GIMS GLOBAL GMBR GMQADMIN GMQQUEUE GSDSF GXFACILI HCICSFCT
                 IBR$HIM IIMS JAMES JCICSJCT JIMS KCICSJCT LIMS LOGSTRM
                 MCEXPPPT MCICSPPT MIMS MQADMIN MQQUEUE NCEXPPPT NCICSPPT
                 OPERCMDS PARTEN@N PCICSPSB PTKTDATA PTKTVAL QCICSPSB
                 RACFVARS RCICSRES RIMS RRSFDATA RVARSMBR SCICSTST SDSF
                 SERVAUTH SERVER STARTED SURROGAT TCICSTRN TIMS TSOAUTH
                 TSOPROC UCICSTST UNIXMAP UNIXPRIV VCICSCMD WCICSRES WILKO
                 XFACILIT
GENERIC PROFILE CLASSES =  DATASET ACCTNUM ACICSPCT AIMS ALCSAUTH ANDY
                           APPCLU APPCPORT APPCSERV APPCSI APPCTP APPL
                           CACHECLS CBIND CCICSCMD CIMS CONSOLE CPSMOBJ
                           CPSMXMP CP1$TPL CP1TPL CRYPTOZ CSFKEYS CSFSERV
                           DASDVOL DBNFORM DCEUUIDS DCICSDCT DEVICES DIGTCERT
                           DIGTCRIT DIGTNMAP DIGTRING DIRACC DIRAUTH DIRECTRY
                           DIRSRCH DLFCLASS DSNADM DSNR EJBROLE FACILITY
                           FCICSFCT FIELD FILE FIMS FSACCESS FSOBJ FSSEC
                           GMBR IBMOPC IBR$HIM IIMS ILMADMIN INFOMAN IPCOBJ
                           JAMES JAN JAVA JCICSJCT JESINPUT JESJOBS JESSPOOL
                           KEYSMSTR LDAP LDAPBIND LFSCLASS LIMS LOGSTRM
***
```

```
PASSWORD
PASSWORD
MIXED CA
SPECIAL (
 6 GENERA                                                NTAINED.
AFTER   :                                                TEMPTS,
    A US
PASSWORD
NO INSTA                                                 ENT.
```

RACF Utilities

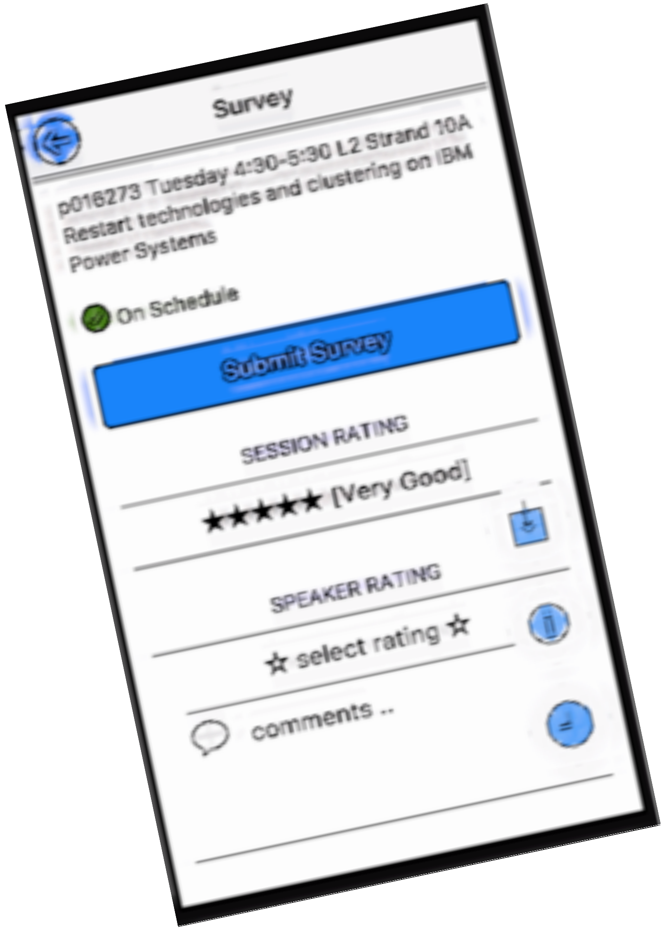
IRRMIN00	Database initialisation
IRRUT100	Cross reference
IRRUT200	Database verification & copy
BLKUPD	Block update
IRRUT400	Database split/merge/extend
IRRDBU00	Database unload
IRRRID00	Remove ID utility
IRRADU00	SMF data unload
RACFRW	RACF report writer
DSMON	Data security monitor

Summary

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
- Many RACF utilities ……

Please complete the session survey!



Survey

p016273 Tuesday 4:30-5:30 L2 Strand 10A Restart technologies and clustering on IBM Power Systems

On Schedule

Submit Survey

SESSION RATING

★★★★★ [Very Good]

SPEAKER RATING

☆ select rating ☆

comments ..

Contact

Leanne Wilson
RSM Partners
leannew@rsmpartners.com
mobile: +44 (0) 7854 590416
www.rsmpartners.com