#SHAREorg

How to Monitor and Assure your z Security Status

Simon Dodge, zSeries Security Principal Engineer
WellsFargo Bank

Tuesday, 13 March, 2012
Session 10450

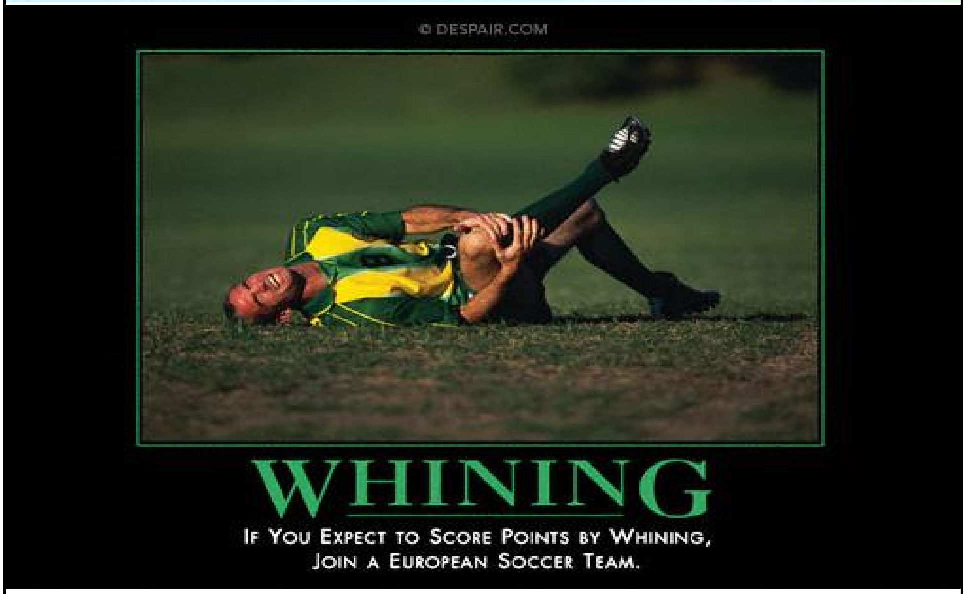
Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

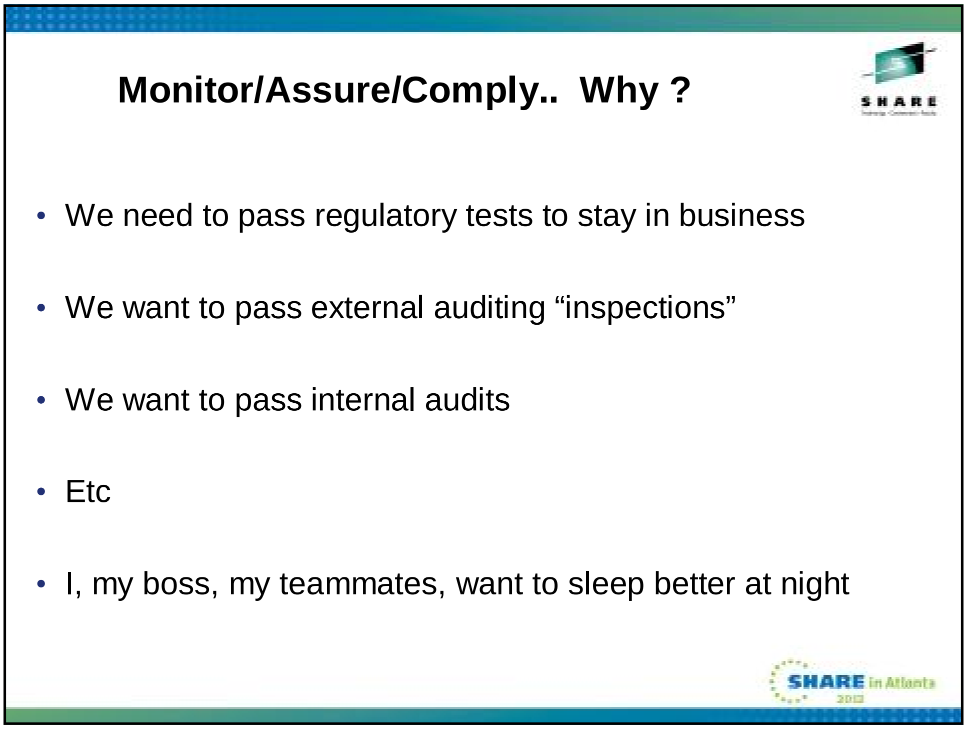
WellsFargo facts

- 70 M customers
- 9K Stores; 12K ATMs
- 20M Online Banking customers
- 7M mobile customers
- A WellsFargo location within 2 miles of 50% of Americans
- 250K+ MIPS
- CICS daily transaction volume: 625M average, 935M peak

Topics

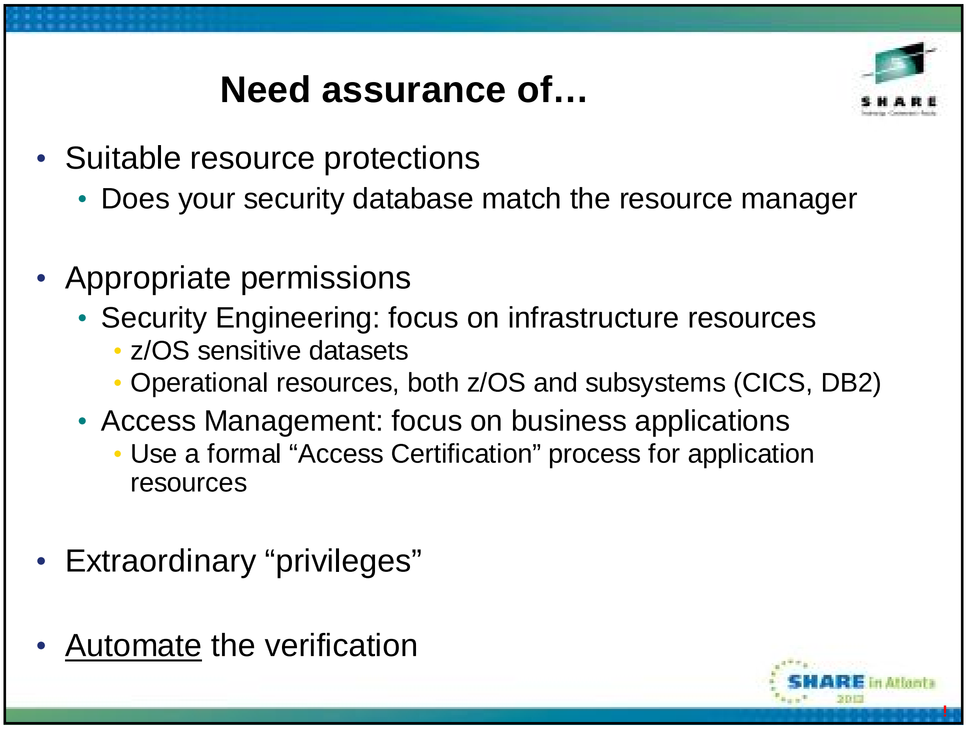
- Monitoring / Self Audit / Self Assessment / Compliance
- Applying Administrative constraints / Enforcing administrative policies
- Privilege Classifications
- Regression testing


© DESPAIR.COM
WHINING
If You Expect to Score Points by Whining, Join a European Soccer Team.



Monitor/Assure/Comply.. Why ?

- We need to pass regulatory tests to stay in business
- We want to pass external auditing “inspections”
- We want to pass internal audits
- Etc
- I, my boss, my teammates, want to sleep better at night



Need assurance of…

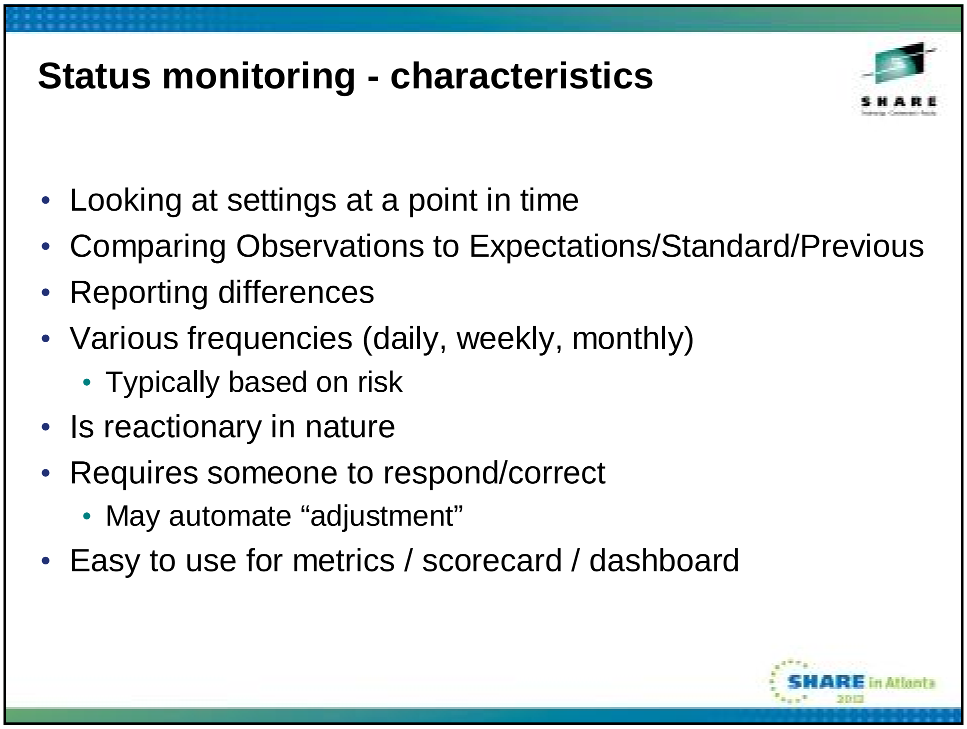
- Suitable resource protections
  - Does your security database match the resource manager
- Appropriate permissions
  - Security Engineering: focus on infrastructure resources
    - z/OS sensitive datasets
    - Operational resources, both z/OS and subsystems (CICS, DB2)
  - Access Management: focus on business applications
    - Use a formal “Access Certification” process for application resources
- Extraordinary “privileges”
- Automate the verification

Self Audit / Health Check

- Consider investing in a vendor audit tool
- Avoid repetitive human involvement
  - Be careful about making the process too bureaucratic
  - The less human involvement, the more frequently you can run it
- Continually revise and add to this process
- Consider different reporting frequencies
  - Based on risk
  - As you go up the management chain

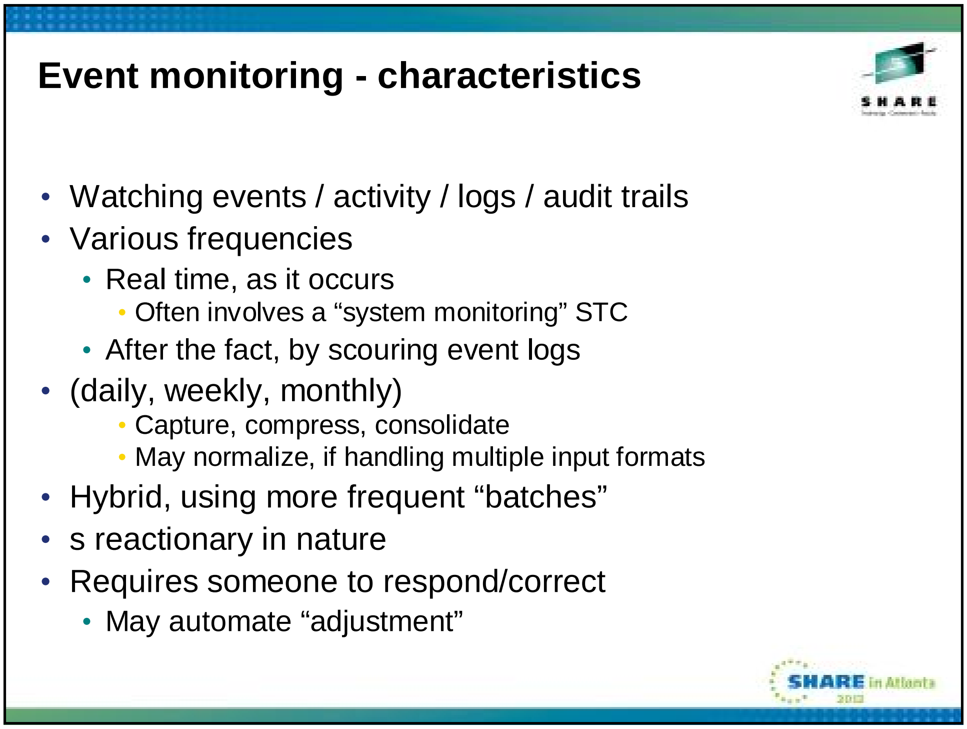
Status –vs- Event monitoring

- Status monitoring inspects a setting / value
  - Like taking an inventory in a store
  - Will not catch a Change + Undo in same interval
- Event monitoring watches events – actual activity
  - Like watching the shoppers in a store
  - Could be just audited events (ESM audit settings)
  - Could be all events (needs exits, or front ending SVC’s)
  - Does not see the whole picture, such as unused permissions
  - Nor unprotected resources (until they are accessed)
- Many folks settle on one approach, however neither is an adequate solution



Status monitoring - characteristics

- Looking at settings at a point in time
- Comparing Observations to Expectations/Standard/Previous
- Reporting differences
- Various frequencies (daily, weekly, monthly)
  - Typically based on risk
- Is reactionary in nature
- Requires someone to respond/correct
  - May automate “adjustment”
- Easy to use for metrics / scorecard / dashboard

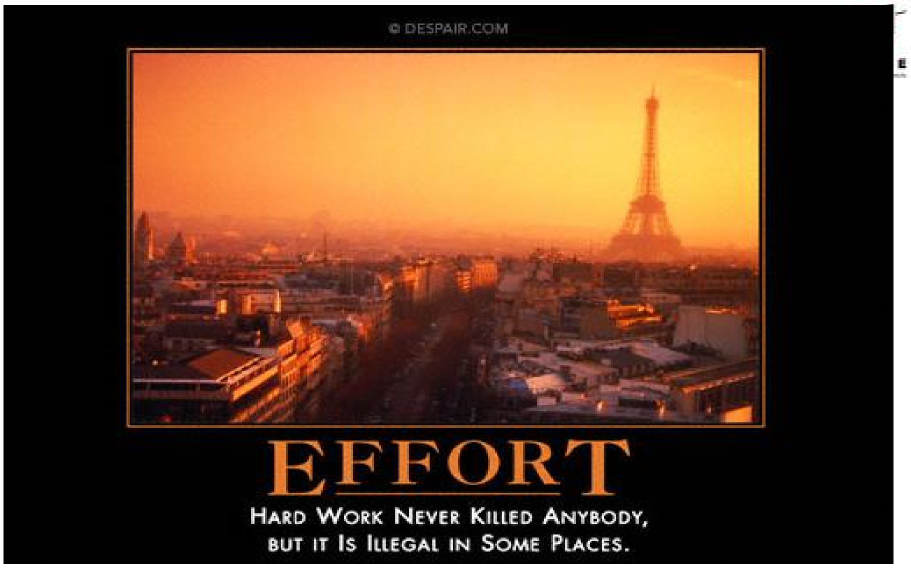


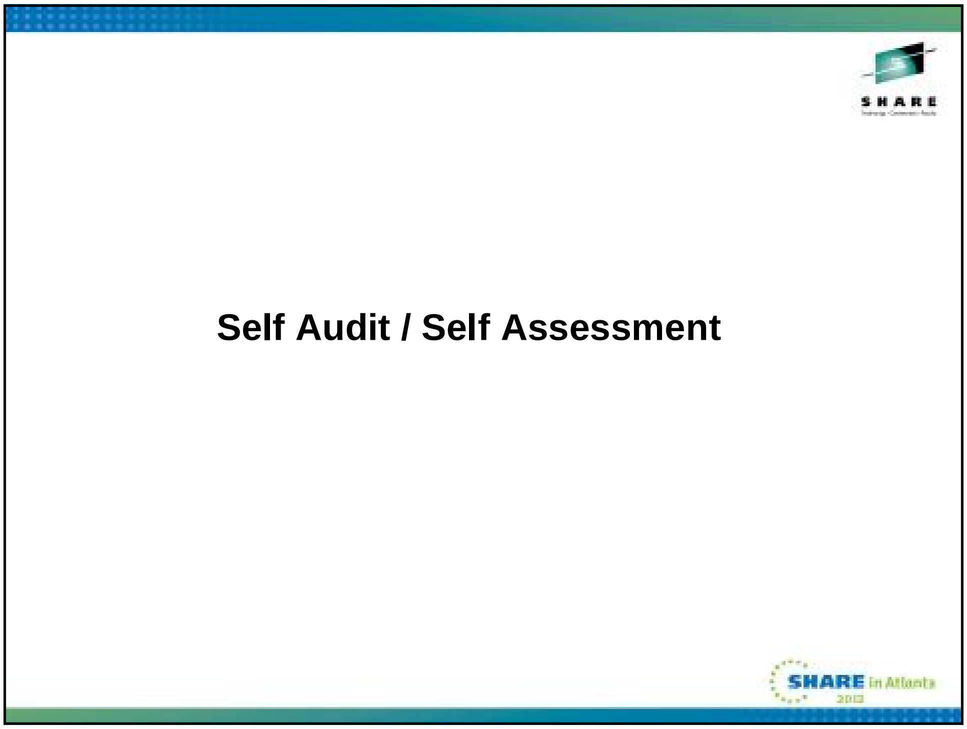
Event monitoring - characteristics

- Watching events / activity / logs / audit trails
- Various frequencies
  - Real time, as it occurs
    - Often involves a “system monitoring” STC
  - After the fact, by scouring event logs
- (daily, weekly, monthly)
    - Capture, compress, consolidate
    - May normalize, if handling multiple input formats
- Hybrid, using more frequent “batches”
- s reactionary in nature
- Requires someone to respond/correct
  - May automate “adjustment”

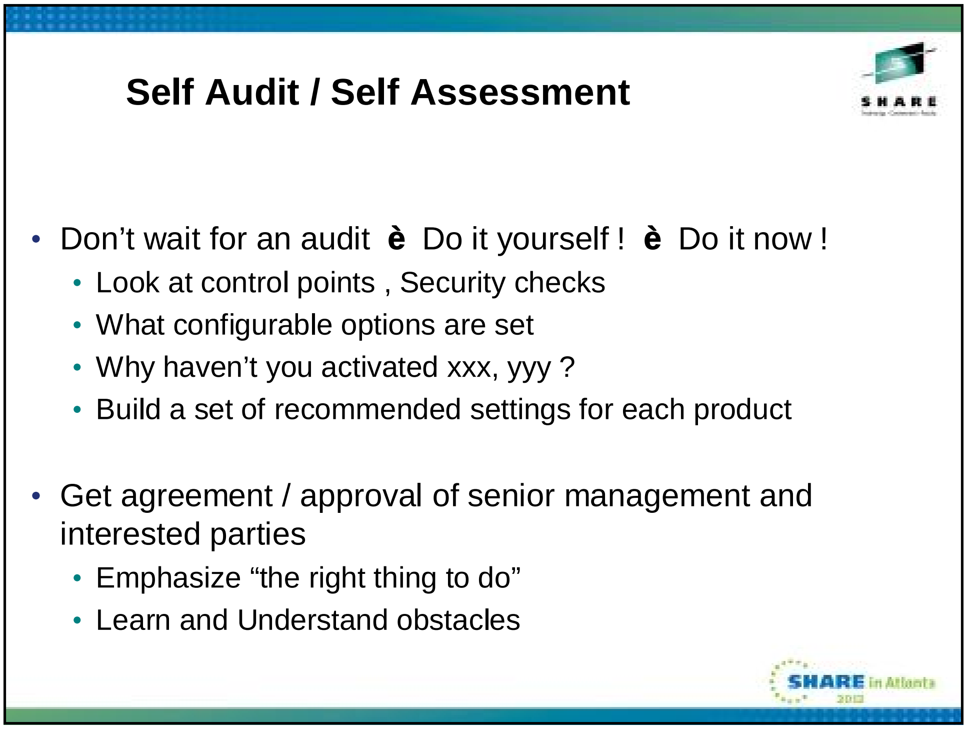
Self Audit / Self Assessment

- Where are you today ?
- Where do you want to be ?
- Develop a remediation plan to get there
  - Design a solution
    - Get agreement / approval
  - Plan an implementation
    - Get agreement / approval
  - Remediate
    - Get acknowledgment when complete
- Implement a compliance check to verify no regression
- Repeat, continuously


© DESPAIR.COM
EFFORT
Hard Work Never Killed Anybody,
but it Is Illegal in Some Places.

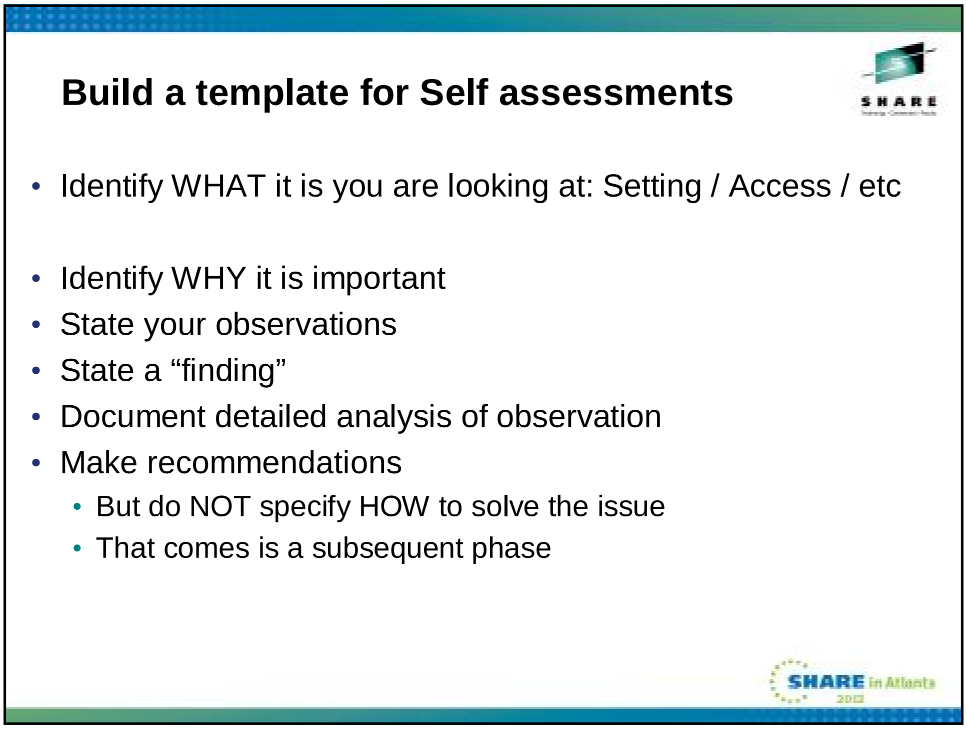


Self Audit / Self Assessment



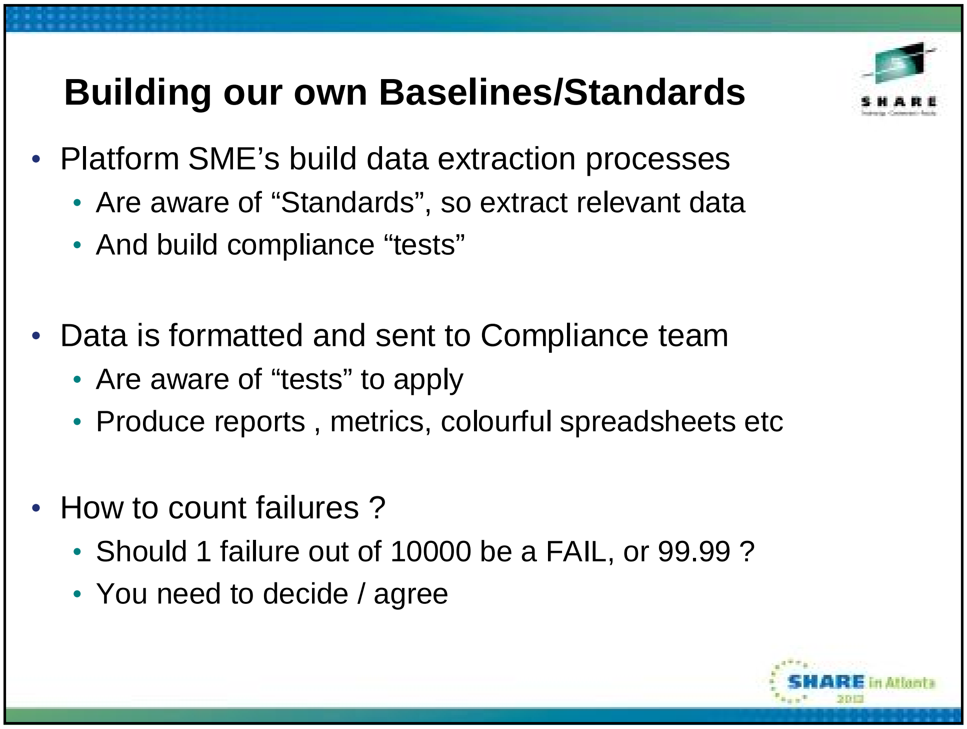
Self Audit / Self Assessment

- Don’t wait for an audit è Do it yourself ! è Do it now !
  - Look at control points , Security checks
  - What configurable options are set
  - Why haven’t you activated xxx, yyy ?
  - Build a set of recommended settings for each product
- Get agreement / approval of senior management and interested parties
  - Emphasize “the right thing to do”
  - Learn and Understand obstacles



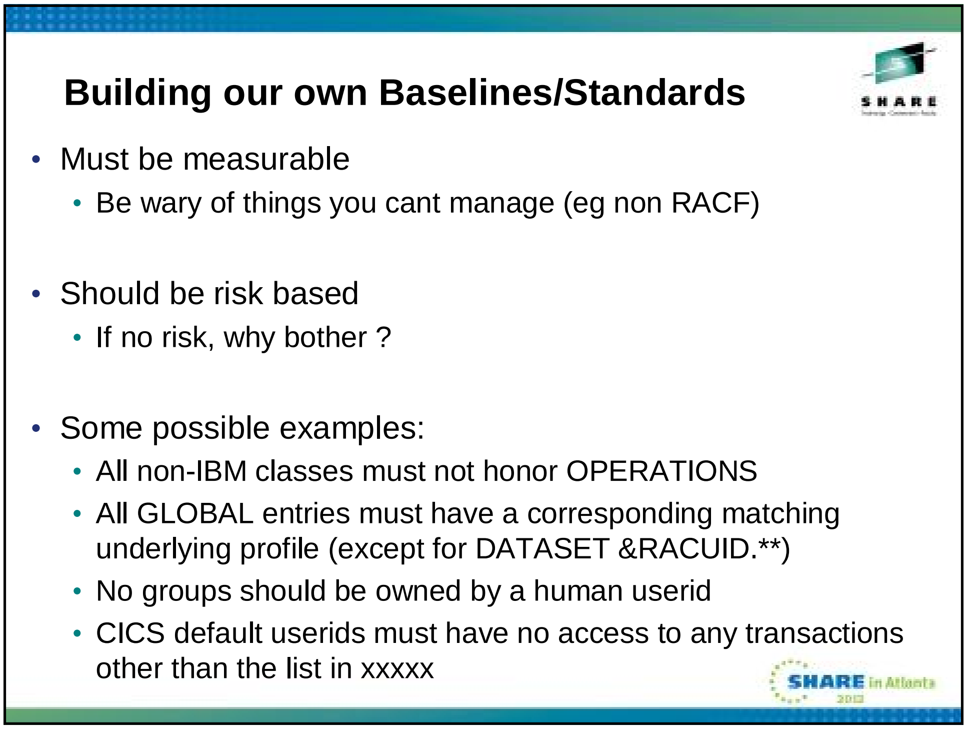
Build a template for Self assessments

- Identify WHAT it is you are looking at: Setting / Access / etc
- Identify WHY it is important
- State your observations
- State a “finding”
- Document detailed analysis of observation
- Make recommendations
  - But do NOT specify HOW to solve the issue
  - That comes is a subsequent phase



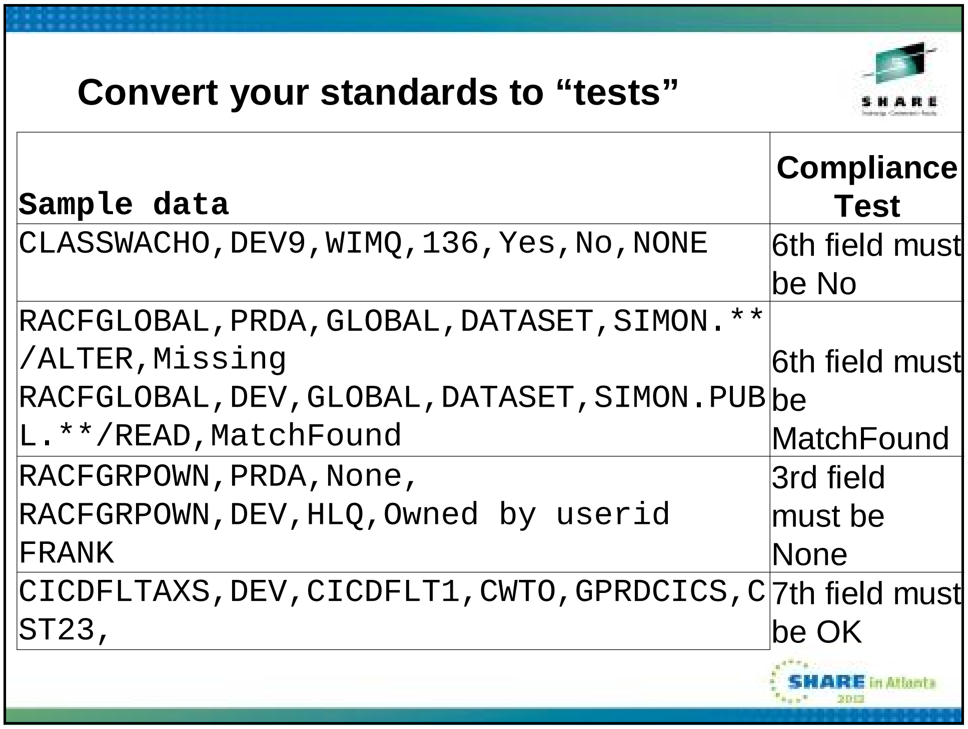
Building our own Baselines/Standards

- Platform SME’s build data extraction processes
  - Are aware of “Standards”, so extract relevant data
  - And build compliance “tests”
- Data is formatted and sent to Compliance team
  - Are aware of “tests” to apply
  - Produce reports , metrics, colourful spreadsheets etc
- How to count failures ?
  - Should 1 failure out of 10000 be a FAIL, or 99.99 ?
  - You need to decide / agree



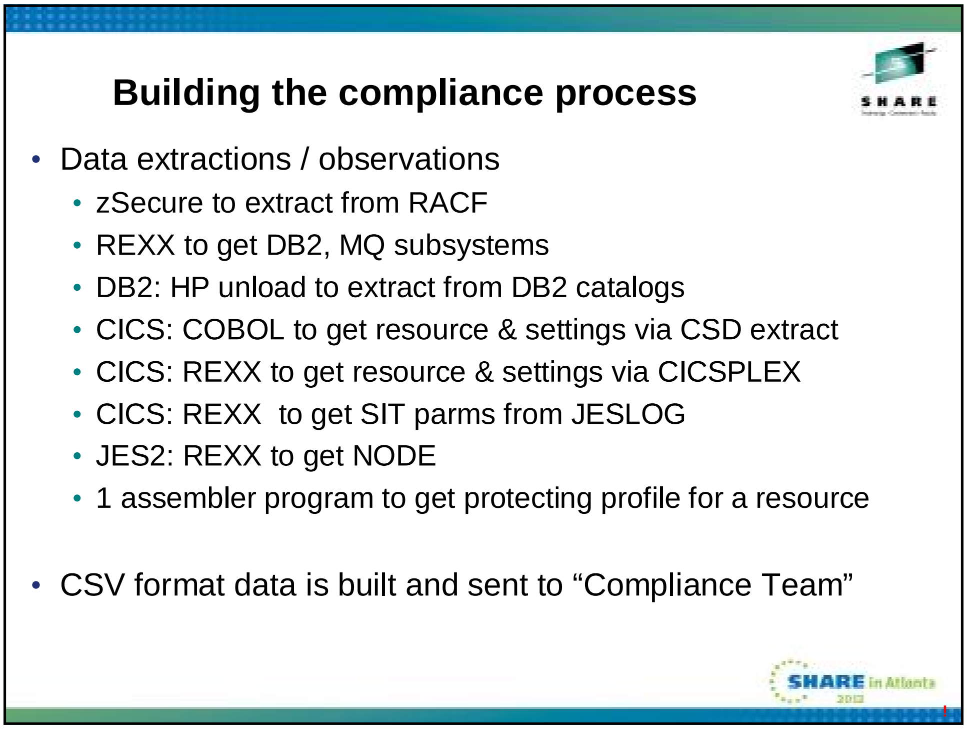
Building our own Baselines/Standards

- Must be measurable
  - Be wary of things you cant manage (eg non RACF)
- Should be risk based
  - If no risk, why bother ?
- Some possible examples:
  - All non-IBM classes must not honor OPERATIONS
  - All GLOBAL entries must have a corresponding matching underlying profile (except for DATASET &RACUID.**)
  - No groups should be owned by a human userid
  - CICS default userids must have no access to any transactions other than the list in xxxxx



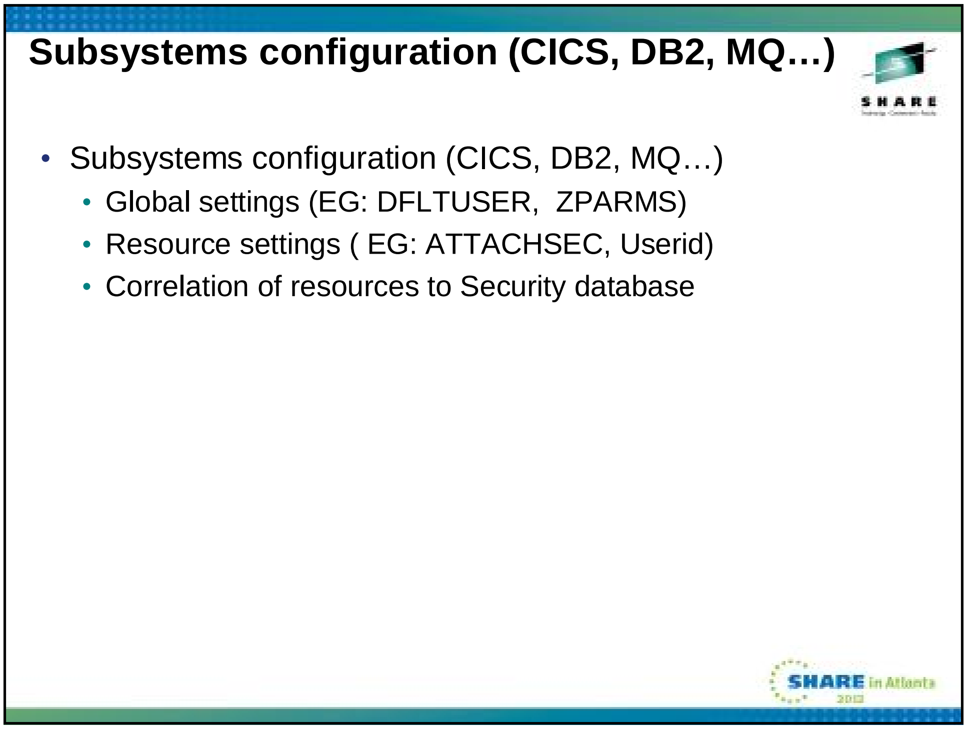
Convert your standards to “tests”

Sample data	**Compliance Test**
CLASSWACHO,DEV9,WIMQ,136,Yes,No,NONE	6th field must be No
RACFGLOBAL,PRDA,GLOBAL,DATASET,SIMON.**/ALTER,Missing RACFGLOBAL,DEV,GLOBAL,DATASET,SIMON.PUBL.**/READ,MatchFound	6th field must be MatchFound
RACFGRPOWN,PRDA,None, RACFGRPOWN,DEV,HLQ,Owned by userid FRANK	3rd field must be None
CICDFLTAXS,DEV,CICDFLT1,CWTO,GPRDCICS,CST23,	7th field must be OK



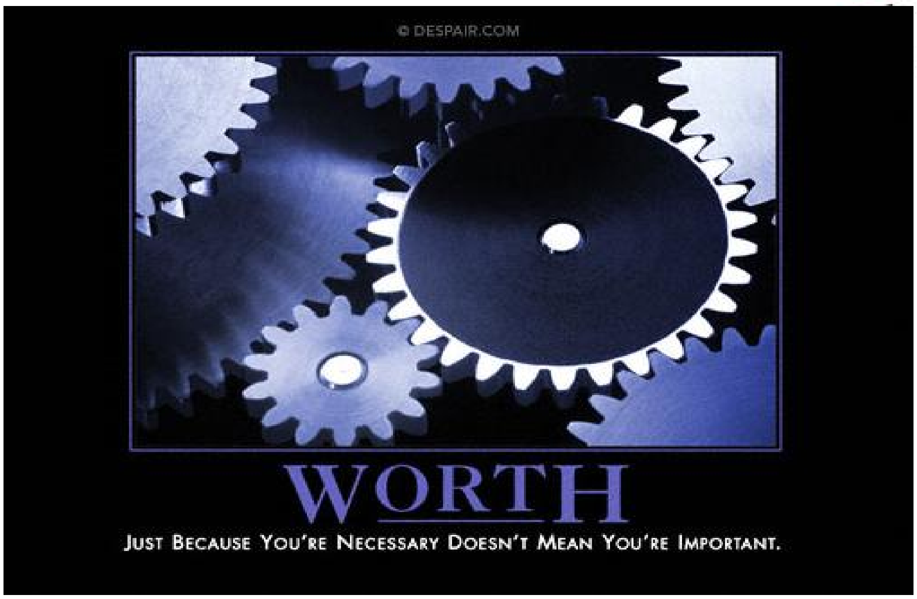
Building the compliance process

- Data extractions / observations
  - zSecure to extract from RACF
  - REXX to get DB2, MQ subsystems
  - DB2: HP unload to extract from DB2 catalogs
  - CICS: COBOL to get resource & settings via CSD extract
  - CICS: REXX to get resource & settings via CICSPLEX
  - CICS: REXX to get SIT parms from JESLOG
  - JES2: REXX to get NODE
  - 1 assembler program to get protecting profile for a resource
- CSV format data is built and sent to “Compliance Team”



Subsystems configuration (CICS, DB2, MQ…)

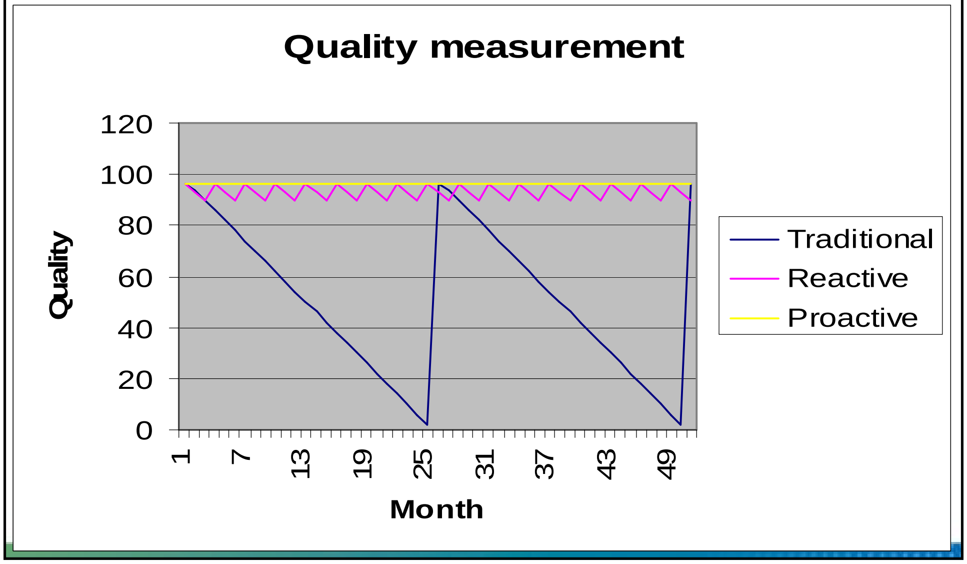
- Subsystems configuration (CICS, DB2, MQ…)
  - Global settings (EG: DFLTUSER, ZPARMS)
  - Resource settings (EG: ATTACHSEC, Userid)
  - Correlation of resources to Security database



© DESPAIR.COM
WORTH
JUST BECAUSE YOU'RE NECESSARY DOESN'T MEAN YOU'RE IMPORTANT.

Applying Administrative constraints / Enforcing policies

Which line represents YOU ?



Administrative controls: Command Verifier

- Intercept all RACF commands

- Applies additional layer of control (“policies”)
- Can validate content of command
- Can override RACF defaults (EG OWNER)
- Can insert missing keywords (EG FROM(xxxxx))
- Can provide live audit trail

Examples

```
connect AMUN group(share) special

C4R551E GrpSpecial attribute not allowed, command
terminated
```

```
permit ‘RA.**' id(stcca7) access(read)

C4R601E ACL setting STCCA7 READ not allowed, command
terminated
```

```
addsd 'ANUBIS.discrete'

C4R613E DISCRETE profiles not allowed, command terminated
```

```
addsd ‘ISIS.TMP.*.**'

C4R640E Define/Delete DATASET ISIS.TMP.*.** not allowed,
command terminated
```

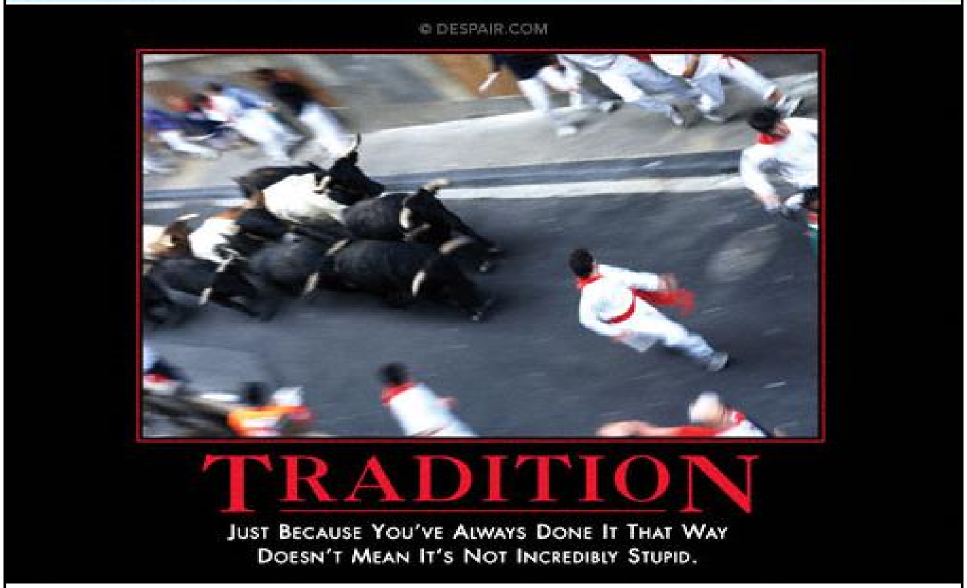
Sample audit trail 1 of 2

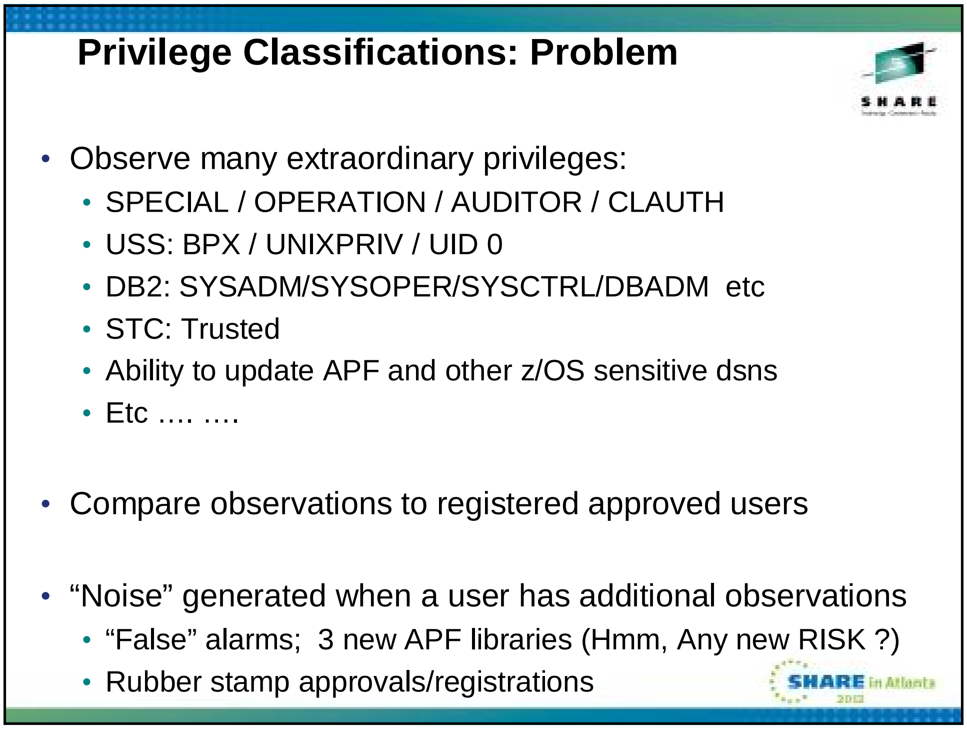
```
USER=ANUBIS  NAME=GUESS WHO             OWNER=SECADMIN
  CREATED=03.232
… Lines snipped …
SECURITY-LABEL=NONE SPECIFIED
C4R736I Command Audit Trail for USER ANUBIS
C4R739I Segment:  CICS    Added on 06.087/16:28 by SEKHMET
C4R739I           OMVS    Added on 08.053/10:10 by ODIN
C4R739I           WORK    Added on 06.087/16:29 by SEKHMET
C4R739I Attrib:   UAUDIT  Removed on 07.332/15:06 by ODIN
C4R739I                   Added on 07.332/14:21 by GEB
C4R739I           AUDITOR Removed on 07.313/10:33 by ODIN
C4R739I                   Added on 07.303/11:37 by GEB
C4R739I           PASSWRD Added on 06.283/15:53 by ISIS
C4R739I           RESUME  Added on 06.283/15:54 by ISIS
C4R739I           OWNER   Changed on 08.108/09:16 by ISIS
C4R739I           DFLTGRP Changed on 08.108/09:16 by ISIS
C4R739I           NAME    Changed on 08.120/11:19 by NUT
```

Sample audit trail 2 of 2

```
C4R739I Connect:           RC1772 Removed on 07.190/12:39 by ISISU
C4R739I                    SYS1 Removed on 07.213/12:43 by NUT
C4R739I                    @SECLSE Added on 07.298/12:34 by NUT
C4R739I                    EMPL Removed on 07.298/17:26 by NUT
C4R739I                    @TSD Removed on 07.303/10:35 by ANUBIS
C4R739I                    $U21AS Added on 08.108/09:16 by OSIRIS
C4R739I GrpAttr:   SPEC    @TSD Removed on 07.303/10:31 by ANUBIS
C4R739I                    @SECLSE Removed on 07.303/11:22 by ISIS
C4R739I            OPER    @TSD Removed on 07.303/10:31 by ANUBIS
```

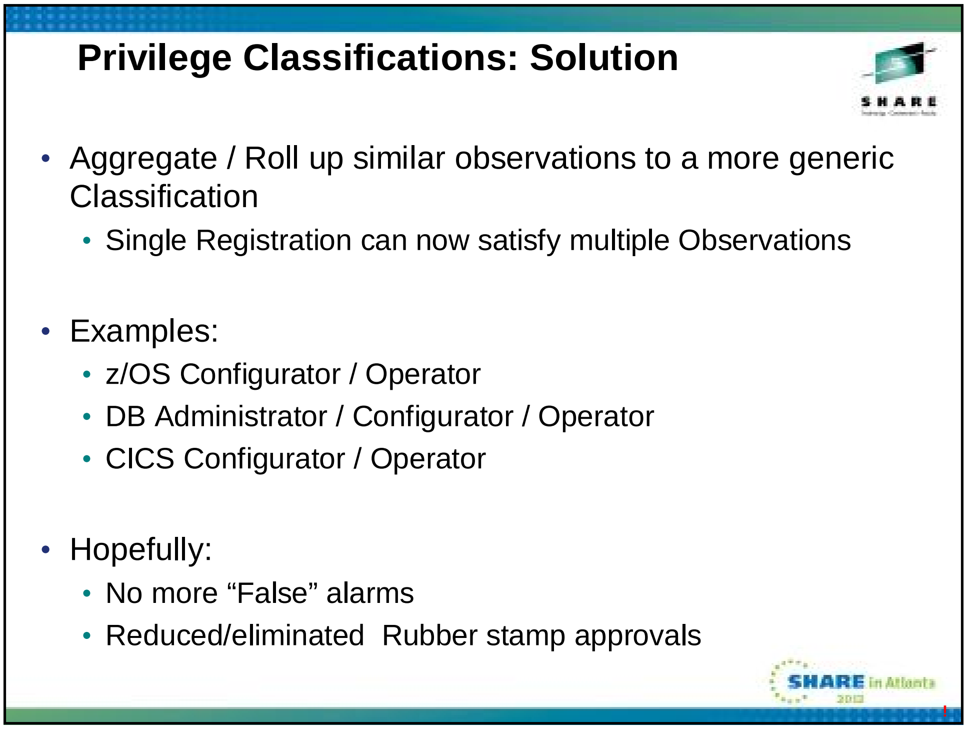
```
C4R736I Command Audit Trail for DATASET  HERA.**
C4R739I Attrib: WARNING Added on 08.072/11:07 by ZEUS
C4R739I                 Removed on 08.072/11:07 by ZEUS
C4R739I Access:         SECLSE access READ on 07.347/10:11 by NUT
C4R739I                 FRED access READ on 08.093/08:56 by ISIS
```


© DESPAIR.COM
TRADITION
JUST BECAUSE YOU'VE ALWAYS DONE IT THAT WAY
DOESN'T MEAN IT'S NOT INCREDIBLY STUPID.



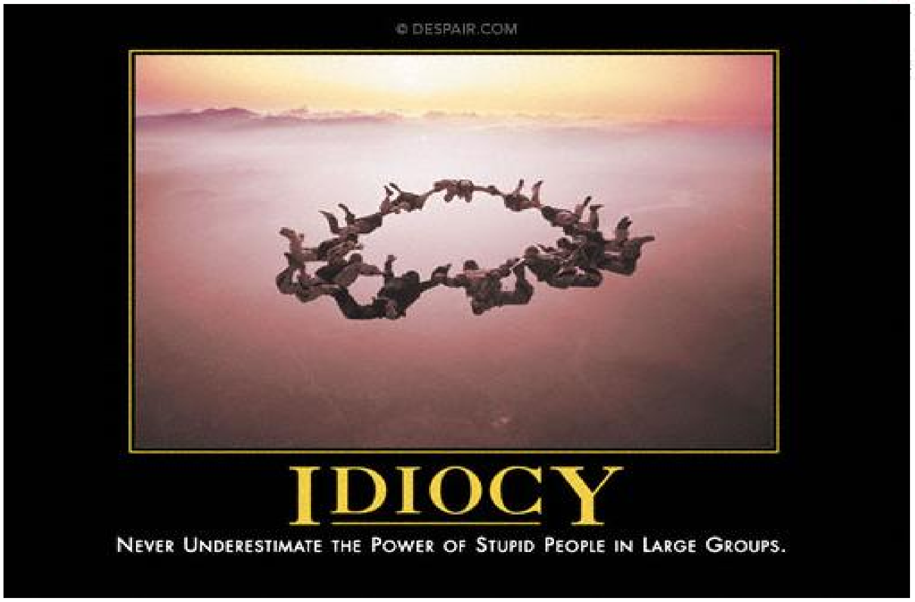
Privilege Classifications: Problem

- Observe many extraordinary privileges:
  - SPECIAL / OPERATION / AUDITOR / CLAUTH
  - USS: BPX / UNIXPRIV / UID 0
  - DB2: SYSADM/SYSOPER/SYSCTRL/DBADM etc
  - STC: Trusted
  - Ability to update APF and other z/OS sensitive dsns
  - Etc …. ….
- Compare observations to registered approved users
- “Noise” generated when a user has additional observations
  - “False” alarms; 3 new APF libraries (Hmm, Any new RISK ?)
  - Rubber stamp approvals/registrations



Privilege Classifications: Solution

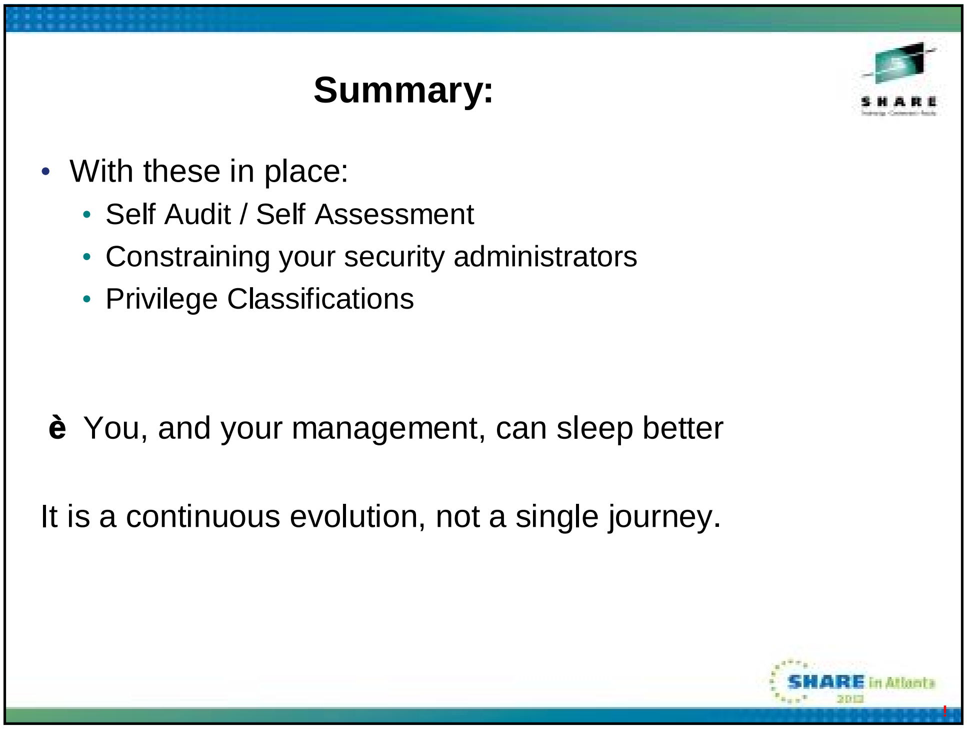
- Aggregate / Roll up similar observations to a more generic Classification
  - Single Registration can now satisfy multiple Observations
- Examples:
  - z/OS Configurator / Operator
  - DB Administrator / Configurator / Operator
  - CICS Configurator / Operator
- Hopefully:
  - No more “False” alarms
  - Reduced/eliminated Rubber stamp approvals


© DESPAIR.COM
IDIOCY
Never Underestimate the Power of Stupid People in Large Groups.

Regression testing.. Quality Assurance

New area to explore: After making RACF changes, can now ask the question..

- Will things still work OK ?
- IE Will users get same RC to same resources ?
- With say a years worth of archived access history, show all differences between RC observed and RC from current RACF db
- Only differences should be a result of your changes
- With all differences explained, you CAN sleep better !!

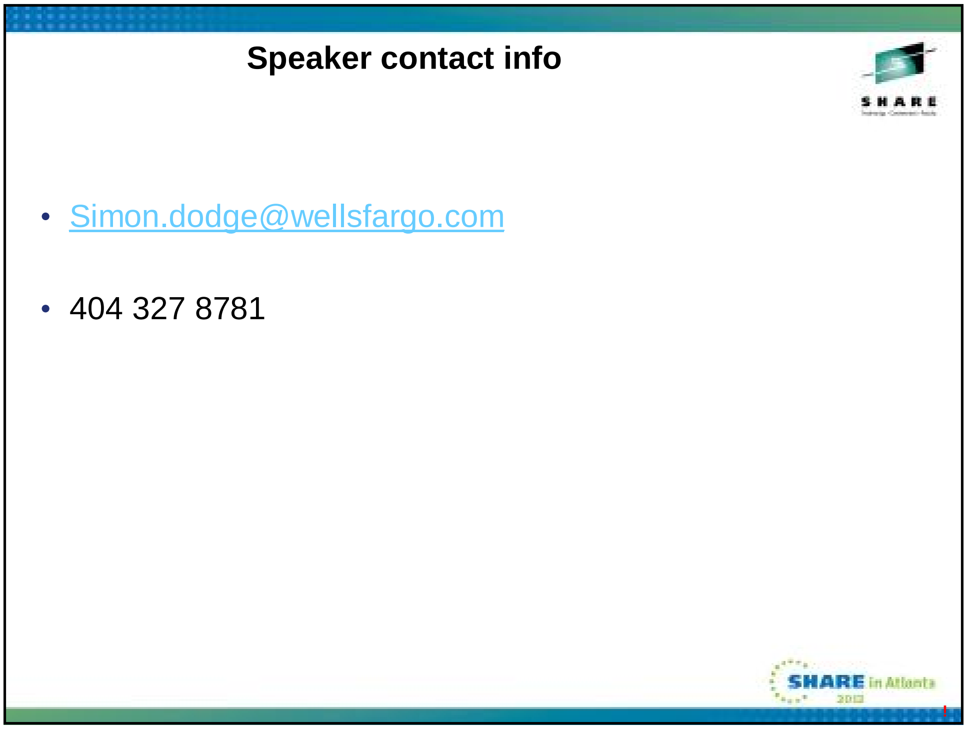


Summary:

- With these in place:
  - Self Audit / Self Assessment
  - Constraining your security administrators
  - Privilege Classifications

è You, and your management, can sleep better

It is a continuous evolution, not a single journey.



Speaker contact info

- Simon.dodge@wellsfargo.com
- 404 327 8781