

IBM®

*Aloha from*

**TIYOLI  
NATION**



# **Mainframe Security War Stories From The Trenches:**

## **AKA - how to avoid a security disaster**

Warning: Contains Technical Material – Parental  
Guidance recommended

Mike Cairns

IBM Tivoli zSecure Technical Specialist

# AGENDA

- PART ONE – the headlines
- PART TWO – the real world issues
- PART THREE – a message from our sponsors
- PART FOUR – Q&A

## PART ONE – the headlines

- Why you came today
- Sensationalism – ‘hackers’ at work!
  - Does happen – potentially high profile – headline grabbing
  - But not very often, and often kept as quiet as possible
- It’s the ‘smaller’ ones that happen day to day are the real concerns

# What's it all about?

- SPECIAL, SPECIAL, SPECIAL...



- Q: Privilege Escalation – how do they do it?
  - A: the standard methods – just like any other system...

## RACF Release Timeline

### September, 1976, Version 1 Release 1

- User identification/verification
- Data set authorization checking
- Journaling
- UT100, UT200, BLKUPD

### July, 1977 Version 1 Release 2

- TAPE and DASD Volume protection
- Dynamic control of RACF options (SETROPTS)
- In-storage index blocks

### July, 1978 Version 1 Release 3

- General resources
- In-storage profiles
- Report Writer (9/80)

### November, 1981 Version 1 Release 4

- Password processing support
- List-of-groups
- RACF data manager interface (ICHEINTY)

## Standard Methods:

- From outside:
  - Enumeration
  - Fingerprinting
  - Vulnerability scanning
  - Pen-test
  - Trojan
- From inside:
  - Accident
  - Malicious
  - Privileged users/administrators



## Standard Responses:

- From outside:
  - But it's a mainframe – no way: Enumeration
  - So what – how does this help them?: Fingerprinting
  - But this is only relevant for users: Vulnerability scanning
  - I trust all my users: Pen-test
  - How exactly?: Trojan
- From inside:
  - We all know this happens: Accident
  - We don't like to think this happens: Malicious
  - We really hope this never happens (to us): Privileged users/administrators

## How about an example?

- Simplest method – Trojan Horse technique:
  - Attack Vectors include:
    - Cataloged Procedure datasets
    - Logon CLISTs and REXX execs
    - Any scripts regularly run by privileged users
- Mitigation:
  - Know the datasets vulnerable to this technique
  - Audit these at the necessary access level
  - Most important – least often performed: Review these Audit Reports!
  - Monitor in real-time

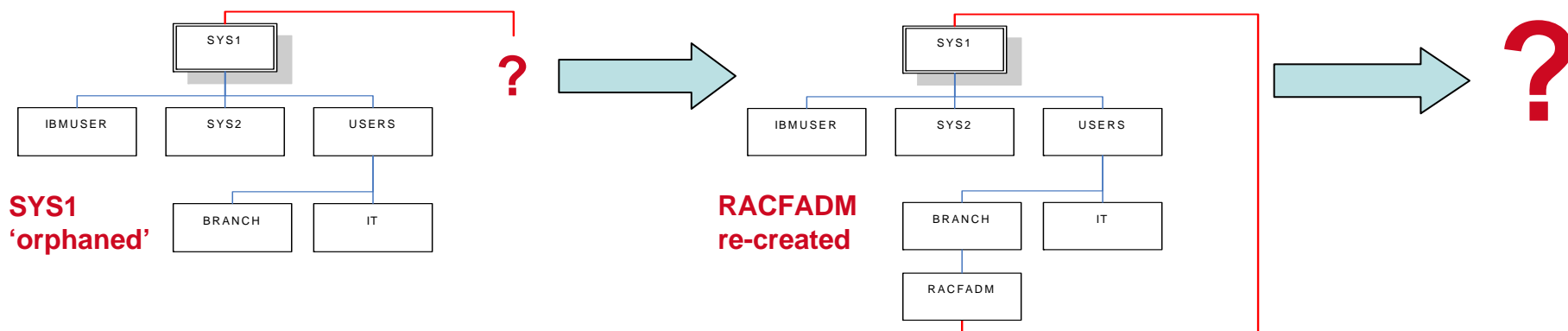
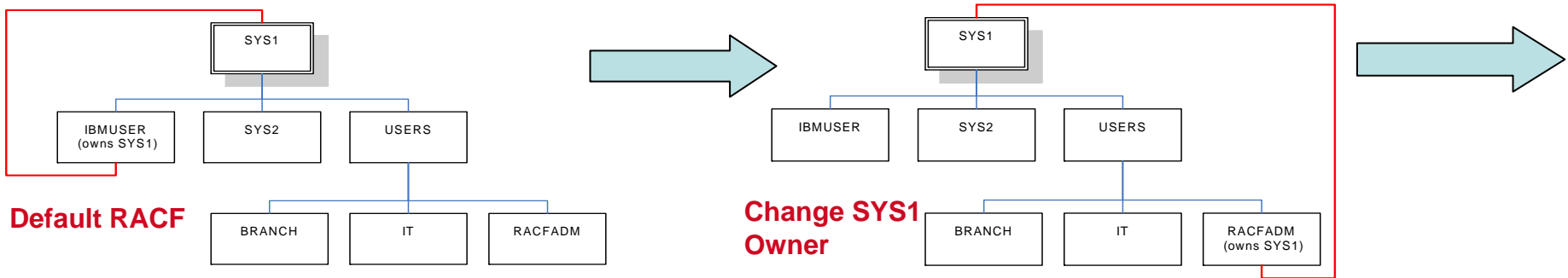


## More technical examples

- The SVC that didn't play nicely:
  - Doesn't validate either its caller, and/or and target data area properly
    - Can be called by anyone with BAS skills – even 'script kiddies' could get relevant code in theory
    - Used by professional z/OS Pen-testers
    - Almost always a method to get SPECIAL this way
- The 'magic SVC' installed for 'maintenance/emergency' use
  - There really is no justification for these nowadays
  - If you really must – then make sure it's internally protected
  - And audit/report on this protection as a priority

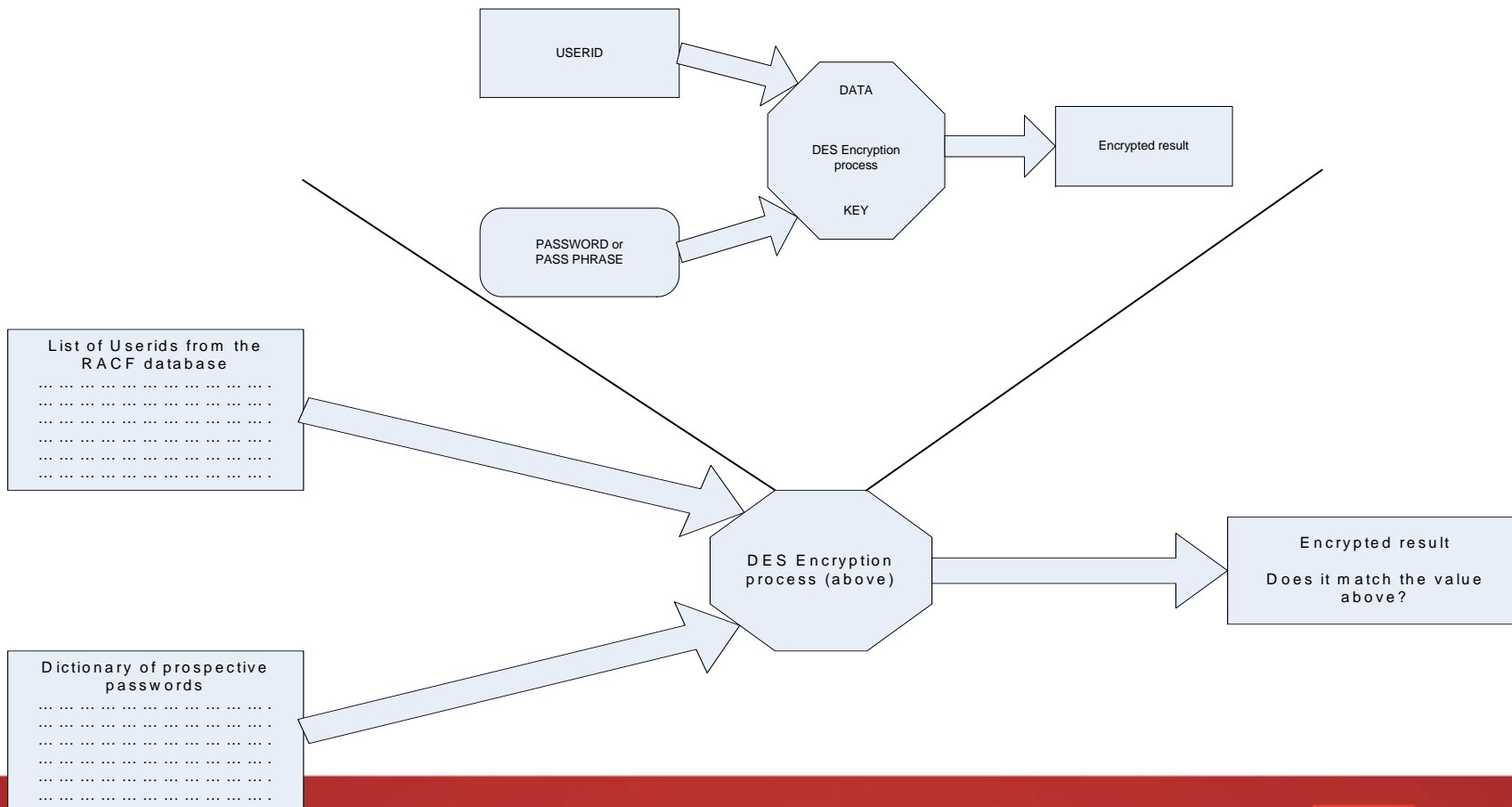
# But it doesn't have to be that technical

- Seemingly minor administrative actions may cumulatively introduce a serious exposure – Group Special example



# The simplest mistake

- READ access to RACF or an exact database copy:
  - Offline brute force attack



## Three avenues for total control of z/OS

- SPECIAL
  - Gimme SPECIAL – Gimme your system... :->
- APF authorisation
  - Update to AFP plus BAS skills is enough – but now you can also download programs that extract passwords from RACF
- Copy of RACF database
  - Brute force offline – opens up both above attacks

## What to do next?

- Our 'hacker':
  - Trojan – wait until I have SPECIAL; he, he, he...
  - SVC attack – get SPECIAL temporarily, grant permanently
  - Group Scope issues – reset a SPECIAL users password
  - Sensitive data in general – discover passwords and config
- Our z/OS security and sysprogs:
  - Trojan – separate logon procs etc for SPECIALs etc
  - SVC attacks – technical z/OS audit and reporting
  - Group Scope issues – control RACF commands
  - Sensitive data in general – data and user classification...

## PART TWO – the real world issues

- Data exposures
- Accidental damage/system errors
- Administrator mistakes
- Security ‘not important’ – must deliver application service no matter what the cost...

## Data scrubbing and job routing example

- Data from production used in test and development jobs
- User able to specify the output class for jobs
- Test system configured to route work to prod if specified
- User submitted test job, routed to prod system, specifying auto-mailer output class.
- Job printed real customer names/addresses, false statement balances, and was automatically sent to Australia Post
- IT executives spend evening in Aussie Post mail sorting room emptying sacks of mail – you don't want that...



## Accidental damage example

- System SPECIAL and AUDITOR activates full SMF auditing for all access
  - System immediately fills SMF datasets
  - Then buffers,
  - Then halts.
- The privileged user again
  - Did they really need that privilege at the time?

# More Accidental damage

- System OPERATIONS
  - Should be entirely unnecessary in modern systems
  - If you must retain it – audit it and control the access with RACF
  - Never on personal userids
  - Move towards STGADMIN RACF control
- Falls into the ‘too much access’ bucket
- IT Sec 101: ‘need to know’
- Segregation of authorities is vital...



# Administrator error damage example

- System Admin deleted all FTP related userids – oops
- Major international bank – all FTP with mainframe down
- Real problem:
  - Easy to recreate the userids and access
  - Hard to restore the passwords to hard coded values
- Lucky in this case – had software that would fix this
  - Zero outage – corrected before problem was noticed

## Delivery over security example

- Batch userids with security administration rights
- Combined with RACF SURROGAT access to these userids by all support staff
- Overall – over 400 staff with the ability to readily ‘hack’
- Large Aussie finance company
- Support staff respond: “We need this access”...
  - Security admin: “All of it?! Full security admin rights as well! For everyone?”

## More Delivery over security

- Major system replacement developed in isolated Ipar
- Shortly before production implementation
  - RACF differences discovered
- 3 month, high risk/profile project to rectify
  - hundreds of thousands of RACF commands issued
- Really a project management and IT governance issue

## What to do next?

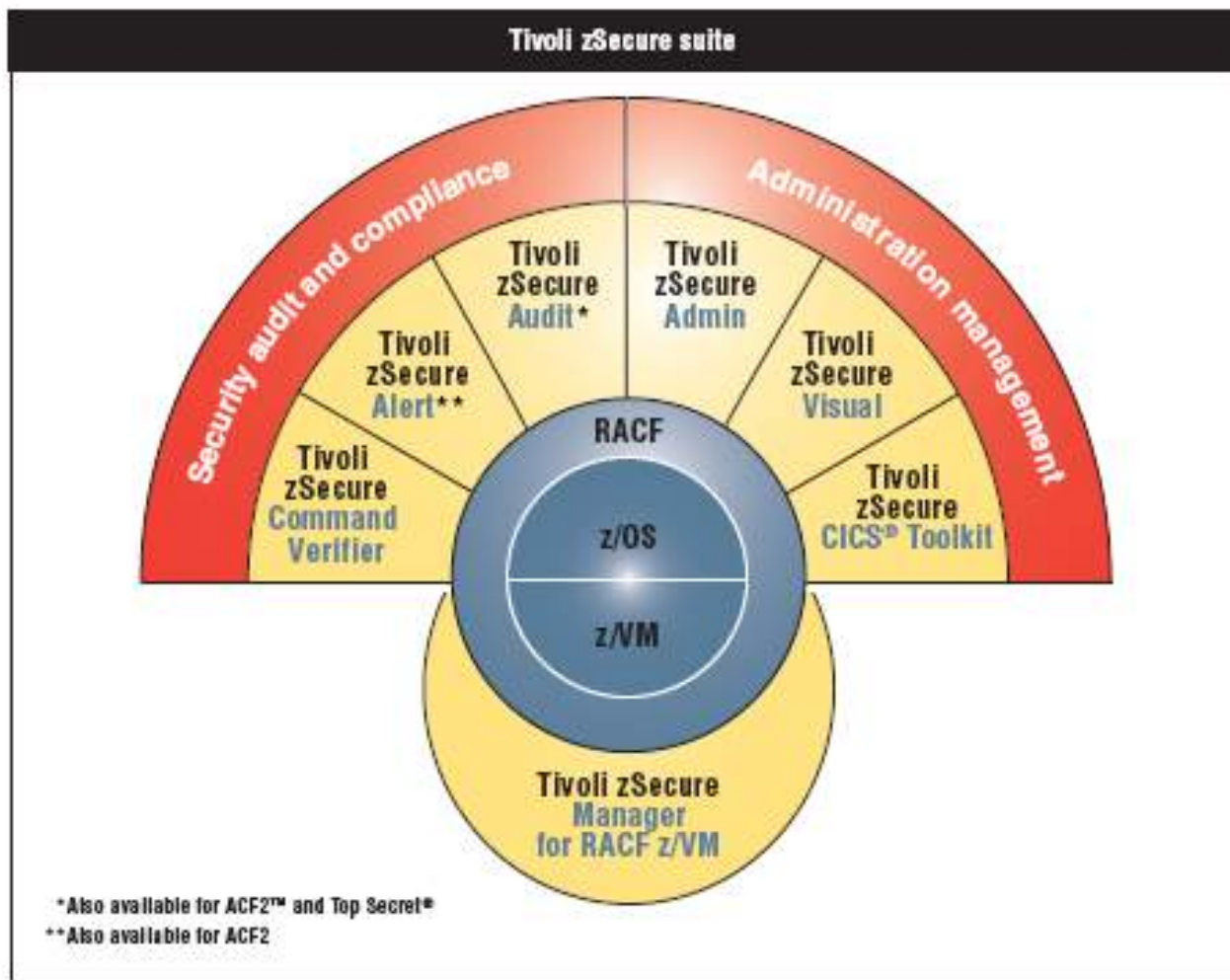
- Data exposures
  - Use real/near-time auditing and monitoring to improve security implementation
- Accidental damage/system errors
  - Segregate the 'killer' access/privileges
- Administrator mistakes
  - See above + automated controls
- Security 'not important' – must deliver application service – no matter what the cost...
  - Business and App Dev governance

# Privacy and confidentiality

- Data classification
  - Classify your data – somehow!
- Role based user access systems
  - Classify your users – provisioning
- Then you can have an ‘access matrix’ – users vs data
- On which you can now implement – Auditing and Monitoring
  - Auditing – once every few months
  - Monitoring – real time



# PART THREE – a word from our sponsors



# Introduction - A bit of Consul history

- 1987 Collect program IOCONFIG version 1 (now zSecure Collect)
  - Collects system snapshot in IOCONFIG file (now CKFREEZE)
- 1989 Consul enters security market with Consul/RACF (now Admin)
  - CARLa command language (somewhat like SAS)
- 1993 Consul/RACF 1.3.0, introduction of Consul/Audit
  - Fully integrated with Consul/RACF from the start
- 1994 Consul/RACF 1.4.0, introduction of CNGRACF component (now CKGRACF)
- 1996 Consul/Command Verification Option for RACF (now Command Verifier)
- 1998 Consul/RACF+Audit 2.3.0, introduction of Consul/Audit for ACF2
- 1998 Consul/RACF Administrator for Windows 1.1 (now Visual)
  - Windows front-end to Consul/RACF
  - Client/server communication shared with Consul/Enterprise (now TCIM)
- 1999 Consul acquires Palace Guard Software, CICS/RACF Toolkit 3.10
- 1999 Consul/Enterprise Audit 2.1 ships OS/390 event source (now TCIM Enabler for z/OS)

# Introduction – Consul zSecure Suite

- 2001 The z/OS era: zSecure name introduced for existing products
  - Version numbers follow z/OS (as Collect had already done for OS/390 for some time)
  - 2001 Consul/zAdmin+zAudit 1.1.0, together called Consul/zSecure
  - 2001 Consul/zVisual 1.1.0
  - 2002 Consul/zLock 1.1.0 (née Command Verification Option)
  - 2002 Consul/zToolkit 1.2.0
- 2003 Version 1.4.5, introduction of Consul/zAlert
  - Alert Address Space does the real-time monitoring
  - Invokes CARLa engine to format and send alerts
- 2005 Version 1.6.0, introduction of Consul zAudit TSS
  - Top Secret support mostly consists of SMF and Audit Tracking File support
  - Product names now without “/”, and “InSight” inserted before zAudit, zAlert, zLock
- 2007 Version 1.8.0, introduction of Consul zAlert ACF2

## Since IBM

- 2007 The Tivoli era: IBM ramps up development and integration
  - Compare Users/Groups function
  - RACF offline
  - CICS SMF type 110 support
  - More z/OS IP Comms Server support
  - DB2 Trace support
  - Tivoli suite integration
  
- Demonstrates tighter integration into z/OS development



# zSecure Admin

```

zSecure RACF USER overview                               1 s elapsed, 0.0 s CPU
Command ==> _____ Scroll==> CSR
Users like ZP*                                          6 Apr 2007 15:45
  User      Complex  Name                DfltGrp  Owner      RIRP  SOA  gC  LCX  Grp
___ ZPU001   MVST    BANKING USER 1     ZPDEPT31 ZPDEPT31   _____  _____  _____  X  2
___ ZPU002   MVST    BANKING USER 2     ZPDEPT31 ZPDEPT31   _____  _____  _____  X  2
___ ZPU003   MVST    BANKING USER 3     ZPDEPT31 ZPDEPT31   _____  _____  _____  X  2
___ ZPU004   MVST    BANKING USER 4     ZPDEPT31 ZPDEPT31   _____  _____  _____  X  2
___ ZPU005   MVST    BANKING USER 5     ZPDEPT31 ZPDEPT31   _____  _____  _____  X  1
___ ZPU006   MVST    BANKING USER 6     ZPDEPT31 ZPDEPT31   _____  _____  _____  X  2
___ ZPU007   MVST    BANKING USER 7     ZPDEPT31 ZPDEPT31   _____  _____  _____  X  2
___ ZPU008   MVST    BANKING USER 8     ZPDEPT31 ZPDEPT31   _____  _____  _____  X  1
___ ZPU009   MVST    BANKING AUDITOR    ZPDEPT31 ZPDEPT31   _____  _____  g          X  3
___ ZPU011   MVST    HR USER 1          ZPDEPT32 ZPDEPT32   _____  _____  _____  X  2
___ ZPU012   MVST    HR USER 2          ZPDEPT32 ZPDEPT32   _____  _____  _____  X  2
___ ZPU013   MVST    HR USER 3          ZPDEPT32 ZPDEPT32   _____  _____  _____  X  3
___ ZPU014   MVST    HR USER 4          ZPDEPT32 ZPDEPT32   _____  _____  _____  X  3
___ ZPU015   MVST    HR USER 5          ZPDEPT32 ZPDEPT32   _____  _____  _____  X  3
___ ZPU016   MVST    HR USER 6          ZPDEPT32 ZPDEPT32   _____  _____  _____  X  3
___ ZPU017   MVST    HR USER 7          ZPDEPT32 ZPDEPT32   _____  _____  _____  X  3
___ ZPU018   MVST    HR USER 8          ZPDEPT32 ZPDEPT32   _____  _____  _____  X  2
___ ZPU019   MVST    HR AUDITOR         ZPDEPT32 ZPDEPT32   _____  _____  g          X  3
___ ZPU031   MVST    IT SPECIALIST 1    ZPDEPT33 ZPDEPT33   _____  _____  _____  X  2

```

# zSecure Visual

File Edit View Navigate Action Maintenance Window Help

Group tree

Filter: Find Load complete tree

SYS1

- CBLDAPGP
- CMNGRP
- DATASETS
- DB2CT
- DB2RE
- DCEGRP
- DFSGRP
- DRLGRP
- IMWEB
- LICADM
- LOTUSGRP
- NETVGRP
- OMVSGRP
- SMCGRP
- SMP
- SMPE
- SUPPORT
- SYS8
- SYSAUDIT
- C2RSRVG
- CONSULGR
- SYSCTLG
- TTY
- USERIDS
- ADMIN
- ARS
- BPUSER
- CCUSER
- DASADMG
- DMUSERS
- SSHOG
- SYSTEMC

Users \* (56)

Userid	Name	InstData	Owner	DefaultGrp	Revoked	Inactive	Expired	Interval	Attempts	LastConnect	LastPwdChange	Created
SMC0003	STUDENT UK CONTEST		SMCGRP	SMCGRP				120		21-03-2007	21-03-2007	06-11-2006
SMC0016	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0017	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		23-11-2006	15-11-2006	31-10-2006
SMC0032	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		09-12-2006	15-11-2006	09-11-2006
SMC0045	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		22-11-2006	15-11-2006	06-11-2006
SMC0052	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		30-12-2006	15-11-2006	06-11-2006
SMC0066	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		01-01-2007	14-12-2006	09-11-2006
SMC0070	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		13-12-2006	15-11-2006	06-11-2006
SMC0092	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		04-12-2006	15-11-2006	06-11-2006
SMC0094	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0096	STUDEN	Schedules		MCGRP	Revoked		Expired	120		10-11-2006		09-11-2006
SMC0098	STUDEN	Connects		MCGRP	Revoked		Expired	120		15-11-2006	15-11-2006	06-11-2006
SMC0113	STUDEN	Permits		MCGRP	Revoked		Expired	120				09-11-2006
SMC0116	STUDEN	Permits		MCGRP	Revoked		Expired	120		10-11-2006		09-11-2006
SMC0130	STUDEN	Scope...		MCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0134	STUDEN			MCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0164	STUDEN	Duplicate...		MCGRP	Revoked		Expired	120		31-12-2006	15-11-2006	09-11-2006
SMC0167	STUDEN	Enforce creation of dataset profile		MCGRP	Revoked		Expired	120		31-12-2006	15-11-2006	06-11-2006
SMC0171	STUDEN			MCGRP	Revoked		Expired	120		10-11-2006		09-11-2006
SMC0172	STUDEN	Add Segment...		MCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0254	STUDEN	Delete		MCGRP	Revoked		Expired	120		27-12-2006	15-11-2006	06-11-2006
SMC0290	STUDEN	Resume...		MCGRP	Revoked		Expired	120		24-12-2006	21-11-2006	06-11-2006
SMC0291	STUDEN	Set Password...		MCGRP	Revoked		Expired	120		24-12-2006	18-11-2006	06-11-2006
SMC0297	STUDEN			MCGRP	Revoked		Expired	120				
SMC0298	STUDEN	Connect...		MCGRP	Revoked		Expired	120				
SMC0305	STUDEN	Segments		MCGRP	Revoked		Expired	120				
SMC0309	STUDEN	Properties		MCGRP	Revoked		Expired	120				
SMC0312	STUDEN			MCGRP	Revoked		Expired	120				
SMC0319	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120				
SMC0326	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120				
SMC0363	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120				

Permits of SMC0096 (15)

Class	Profile	ProfType	Access	When	UAcc	Warning	Erase	AuditS	AuditF	ACL count	Owner
APPL	SMC0096	Discrete	Read		None				Read	3	SYS1
Dataset	SMC0096.**	Generic	Owner		None				Read	1	SMC0096
JESSPOOL	TSTMVS01.STC.SMC0096.**	Generic	Alter		None				Read	5	SYS1
MQADMIN	MQ01.QUEUE.SMC0096.**	Generic	Alter		None				Read	3	SYS1
MQQUEUE	MQ01.SMC0096.**	Generic	Alter		None				Read	3	SYS1
OPERCMD5	MVS.CANCEL.STC.SMC0096.**	Generic	Update		None				Read	5	SYS1
OPERCMD5	MVS.CANCEL.TSU.SMC0096	Discrete	Update		None				Read	2	BABEYS
OPERCMD5	MVS.START.STC.SMC0096	Discrete	Update		None				Read	5	SYS1
OPERCMD5	MVS.START.STC.WEBS096	Discrete	Update		None				Read	2	BABEYS
OPERCMD5	MVS.STOP.STC.SMC0096	Discrete	Update		None				Read	5	SYS1
OPERCMD5	MVS.STOP.STC.WEBS096	Discrete	Update		None				Read	2	BABEYS

Find

Class: User

Search: Exact Filter Mask

<<Advanced

Name: contest

Installation data:

Owner:

Default Group:

Revoke status: Any

Attempts: >

Segment: Any

OK Cancel

# zSecure Alert

**Alert: Information access by SPROGJOE on FINANCE data set SHIPPING.VOLUME.MONTHLY - Lotus Notes**

File Edit View Create Actions Text Help

Address [http://searchdatacenter.techtarget.com/tip/0,289483,sid80\\_gci1243691,00.html?tra](http://searchdatacenter.techtarget.com/tip/0,289483,sid80_gci1243691,00.html?tra)

Workspace Rob van Hoboken - zAlert Alert: Information access by...

1 Save And File 2 Save And Close 3 Follow Up 4 Tools 5 Consul

**C2POLICE at DINO**  
 <c2p.PZ00860@consul.nl>  
 15-10-2006 00:46

Please respond to  
 <security@shipping.co  
 m>

To: Data Security <Datasec@shipping.com>  
 cc:  
 bcc:  
 Subject: Alert: Information access by SPROGJOE on FINANCE data set SHIPPING.VOLUME.MONTHLY

Alert: Information access by SPROGJOE on FINANCE data set SHIPPING.VOLUME.MONTHLY  
 FINANCE data set successfully read

Alert id 4101  
 Date and time 15Oct2006 00:45:27.60  
 Data set SHIPPING.VOLUME.MONTHLY  
 Access READ  
 User SPROGJOE JOE KNOWS IT ALL SYSPROC  
 Result Success  
 Job name COPYDEV  
 System ID DINO

Body of message

Untagged Office

***When your mainframe data is crucial enough  
 that you need to know real-time  
 Alerting AND Action!  
 Send WTO to trigger Automated Operations  
 Issue commands autonomously***





# zSecure Alert integration with TSOM (TSIEM)

Dashboard Reports Tools Options Admin Tivoli Security Op

Visuals Window Help

PowerGrid 14:56:05 CHART REFRESH CONFIG

	Src Threat	Dst Threat	Protocol	Src IP	Dst IP	Src Port	Dst Port	Domain	Src Watchlist	Dst Watchlist	EAM Time	Sensor Time	ID
ued SPECIAL command - SPECIAL authority	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					
cess using SECURITY by user without SECUR	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					
ta set access using READALL by user withou	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT			2007/03/19 20:05:49	2007/03/19 20:05:49	
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					
ata set access using NON-CNCL by user wit	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					

http://tutti - Event #5043729343401951233 - Mozilla Firefox: IBM Edition

**Event #5043729343401951233**

Field	Value
<b>EAM Time</b> Time this event was received by the EAM (according to the EAM's clock).	2007-03-19 20:05:49
<b>Sensor Time</b> Time the sensor detected this event (according to the sensor's clock).	2007-03-19 20:05:49
<b>Sensor Name</b> Name of the Sensor that reported this event.	CONSUL
<b>Sensor Type</b> Type of Sensor that reported this event.	zAlert
<b>Protocol</b> Protocol number of the event.	17
<b>Source IP</b> Source address of this event.	0.0.0.0
<b>Destination IP</b> Destination address of this event.	0.0.0.0
<b>Source Port</b> Source port of this event.	0
<b>Destination Port</b> Destination port of this event.	0
<b>Event Type</b> Type of event.	NON_OPERATIONS_USED_OPERATIONS
<b>Event Class</b> Class of event.	20000
<b>User Name</b> User name.	T.Q.B.F.J.O.T.L. DOG
<b>User Context</b> User context.	DINO
<b>Info</b> Additional information associated with this event.	nonOperationsUsedOperations: "eventIntegral = Alert: non-OPERATIONS user IBMUSER accessed data set with OPERATIONS - ..." "eventWhen = 2003-1-23.11:45:39.3.-1:0" "onWhatDSNAME = SOME.DATASET" "onWhatALLOWED = READ" "onWhatINTENT = CONTROL" "whoUSERID = IBMUSER" "whoNAME = T.Q.B.F.J.O.T.L. DOG" "whatDESC = WARNING" "whatJOBNAME = RACF" "whereSYSTEM = DINO"

Done

# zSecure integration with TCIM

**Enterprise Overview** Settings

Events by top event count by "Who" and "on What" from May 16, 2007 till May 22, 2007.

**on What**

on What	Finance	Sales	Managers	Administrators	Marketing	Remote Users	Other	Who
Finance high	High	Low	Low	Low	Low	Low	Low	Low
Finance low	Low	High	Low	Low	Low	Low	Low	Low
Client data	Low	Low	Low	Low	Low	Low	Low	Low
HR data	Low	Low	Low	High	Low	Low	Low	Low
System data	Low	High	Low	Low	Low	Low	Low	Low
Other	Low	Low	Low	Low	Low	Low	High	Low

**Trend graphic** Settings

Percentage of Policy Exceptions from May 16, 2007 till May 22, 2007.

Line graph showing percentage of policy exceptions over time. The y-axis ranges from 0 to 100%. Two horizontal lines are present at approximately 25% and 35%. The data line fluctuates around the 25% line, with a sharp spike to approximately 45% on May 22, 2007.

**Database Overview**

**AggrDb** **SelfAudit**

**Name:** SelfAudit  
**Status:** Database loaded successfully  
**Loading date:** Sun May 13 2007 20:00:53 GMT+02:00  
**Content:** 192.168.88.133 (InSightPortal), INSIGHTTEST (InSight, INSIGHTTEST\INSIGHTTEST (Windows))  
**Automatic policy:** Sun May 13 2007 19:58:27 GMT+02:00  
**User policy:** Sat Jan 01 2000 01:00:00 GMT+01:00

**My reports** Add custom report Export custom reports

**z/OS reports**

Type	Title	Action
Privileged user access		
Warning mode		

# zSecure Audit

Audit concern overview by priority (higher priorities only)

Line 1 of 8407

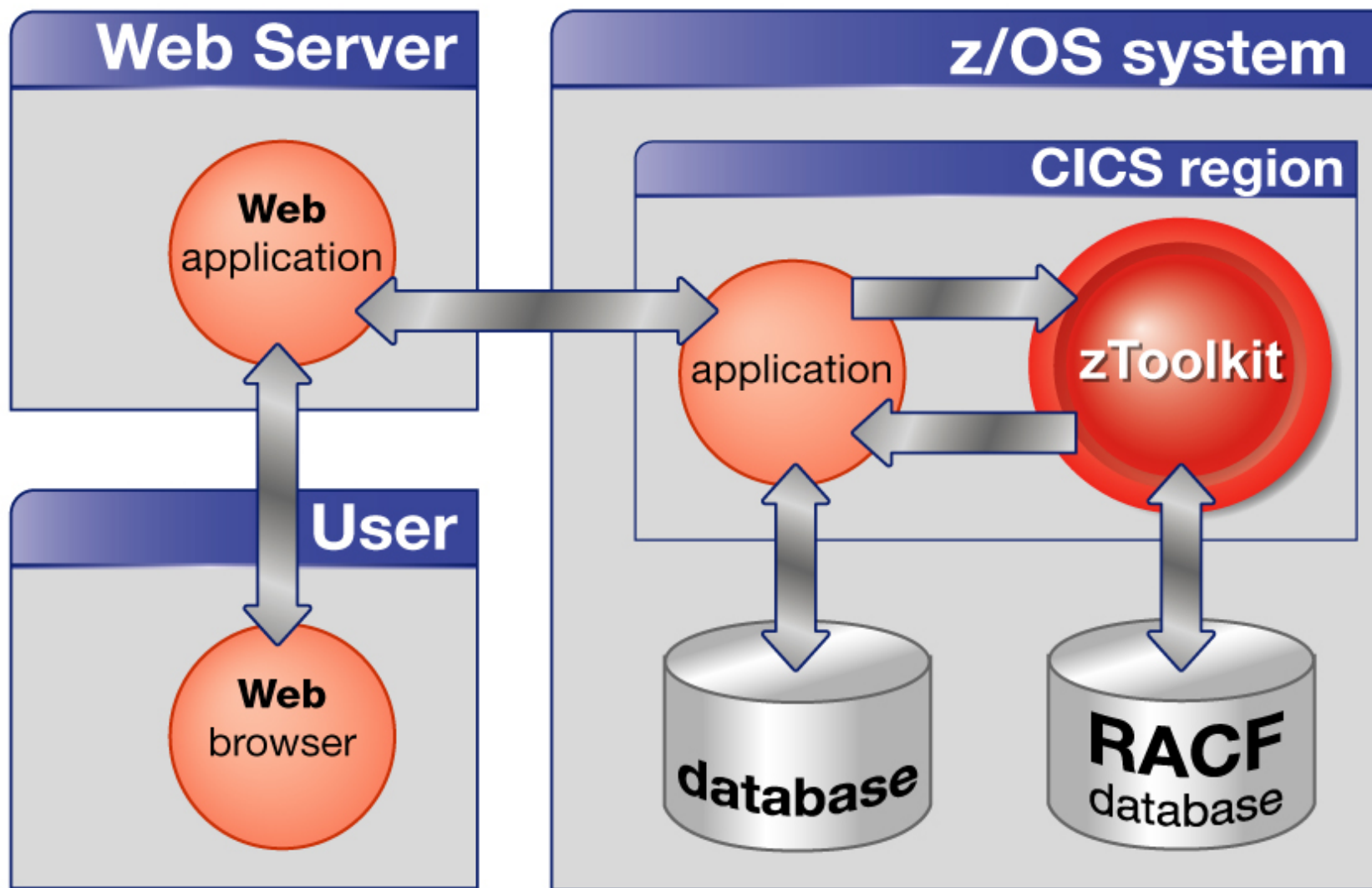
Command ==> \_

Scroll==> CSR

22 Oct 2007 11:59

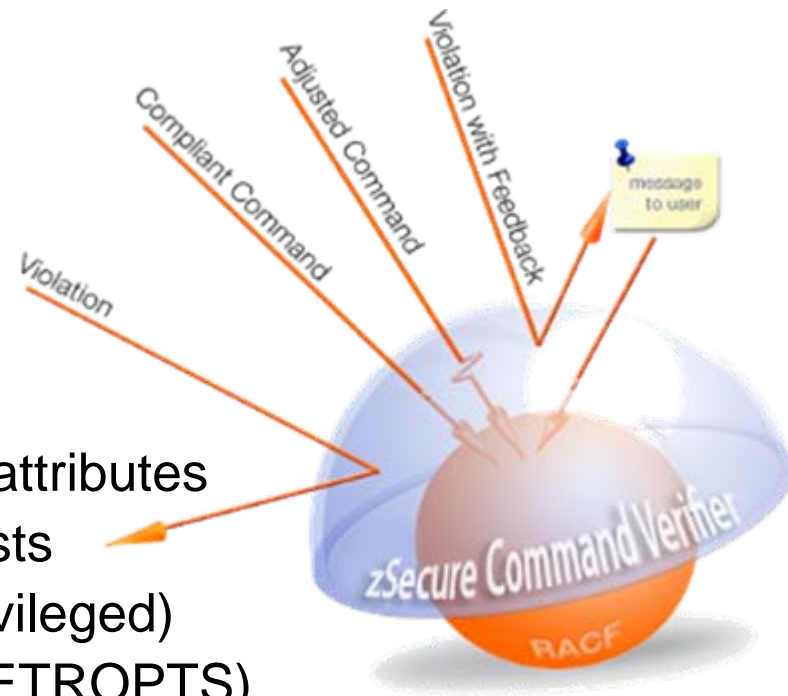
Pri	Complex	Syst	Area	Key	Audit concern
70	RB0DPRIM		SENP	SYS1.**	No read audit, No update audit, UACC too
60	RB0DPRIM		SENP	ICFCAT.**	Unprotected
60	RB0DPRIM		SENP	SYSPROG.**	Unprotected
60	RB0DPRIM		SENP	TIVOLI.**	Unprotected
48	RB0DPRIM	RB0T	TRUS	????????	Superuser authority, can do anything in U
45	RB0DPRIM	RB0T	TRUS	????????	Contains readable passwords and other con
45	RB0DPRIM	RB0T	TRUS	????????	Contains readable passwords and other con
45	RB0DPRIM	RB0T	TRUS	????????	Contains readable passwords and other con
45	RB0DPRIM	RB0T	TRUS	????????	Contains readable passwords and other con
45	RB0DPRIM	RB0T	TRUS	????????	Contains readable passwords and other con
45	RB0DPRIM	RB0T	TRUS	????????	Contains readable passwords and other con
45	RB0DPRIM	RB0T	TRUS	????????	Contains readable passwords and other con
44	RB0DPRIM	RB0T	TRUS	????????	Dictionary or brute force password attack
44	RB0DPRIM	RB0T	TRUS	????????	JES spool may contain readable passwords
44	RB0DPRIM	RB0T	TRUS	????????	May contain readable passwords, even outs
44	RB0DPRIM	RB0T	TRUS	????????	May contain readable passwords, even outs
44	RB0DPRIM	RB0T	TRUS	????????	UADS may contain non-RACF defined TSO use
35	RB0DPRIM	RB0T	SETR	PROTECTAL N	The security system is not even invoked f
23	RB0DPRIM	RB0T	CLAS	APPCSERV	No protection against hackers masqueradin
23	RB0DPRIM	RB0T	CLAS	VTAMAPPL	No protection against hackers masqueradin
22	RB0DPRIM	RB0T	CLAS	DEVICES	Devices like ESCON directors, FEPs, local
20	RB0DPRIM	RB0T	CLAS	DATASET	Profile changes in class are not audited,
20	RB0DPRIM	RB0T	CLAS	TEMPDSN	Temporary datasets resident after failure
20	RB0DPRIM	RB0T	SETR	OPERAUDIT N	OPERATIONS activity undetectable
20	RB0DPRIM	RB0T	SETR	TAPEVOL I	Hacker can read/write any tape dataset by
19	RB0DPRIM	RB0T	CLAS	OPERCMDS	Profile changes in class are not audited
16	RB0DPRIM		RACF	CB.**	Verify why UACC>=UPDATE, Generic chars in
16	RB0DPRIM		RACF	CB.**	Verify why UACC>=UPDATE, Generic chars in

# zSecure CICS Toolkit



## zSecure Command Verifier

- Complete control over all RACF commands (similar to TAMOS)
- Control over command execution
- Enforces installation standards
  - Naming Conventions
  - Defaults for missing values
  - Mandatory values
  - Access Level Standards
  - Elevation of Authority not allowed
    - group special may not pass along attributes
  - Prevent changes to Access Control Lists
  - Prevent use of keywords (Trusted, Privileged)
  - Prevent changes to RACF settings (SETROPTS)
- Optional logging to SMF
- Optional audit trail in RACF profiles





## PART FOUR – Q&A

- Some resources for further information
  - [www.ibmssystemsmag.com](http://www.ibmssystemsmag.com)
    - <http://www.ibmssystemsmag.com/mainframe/julyaugust05/tipstechniques/9785p1.aspx?ht=>
    - <http://www.ibmssystemsmag.com/mainframe/marchapril07/tipstechniques/12532p1.aspx?ht=>
  - Tivoli zSecure software, education and support
    - <http://www-306.ibm.com/software/tivoli/sw-atoz/indexZ.html>
    - [http://www-306.ibm.com/software/tivoli/education/edu\\_prd.html#Z](http://www-306.ibm.com/software/tivoli/education/edu_prd.html#Z)
    - <http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivolizSecureSuite.html>
  - RACF User Group online – RACF-L
    - <http://listserv.uga.edu/archives/racf-l.html>

# Disclaimers and Trademarks

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

The following terms are trademarks or registered trademarks of the IBM Corporation in either the United States, other countries or both: DB2, e-business logo, eServer, IBM, IBM eServer, IBM logo, Lotus, Tivoli, WebSphere, Rational, z/OS, zSeries, System z.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

ITIL® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office.

COBIT® is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute.

ISACA® is a Registered Trade mark of The Information Systems Audit and Control Association

IT Infrastructure Library® is a Registered Trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

IBM, the IBM logo, Candle, CICS, CT, CT/DS, CUA, DB2, eServer, ETE, RACF, IMS, iSeries, MVS, NetView, OMEGAMON, OMEGAMON II, OMEGAVIEW, AIX, Rational, Redbooks, S/390, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, VTAM, Lotus, WebSphere, z/OS, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT® are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries. Other company, product, and service names may be trademarks or service marks of others.