Compensating Controls
aka
How This Systems Programmer Got Her Groove Back!

Julie-Ann Williams
millenia…

August 9, 2011
Session Number: 10103
My life in IT…

- 30 years in IBM Mainframes
- MVS Systems Programmer
  - with Security bias
- Author
  - CICS Essentials
  - z/Auditing Essentials
  - ISV Tech Docs
- Helping Customers to exploit bleeding edge technology on their IBM mainframes
My life on the outside...

• Kat 3 was a wedge-shaped robot with a pneumatic axe
• We competed in Series 2-7 of Robot Wars
• We were extremely proud to win the Series 6 Sportmanship Award
• Originally a double wedge with an overhead axe, the design was changed radically for the 6th series
How This Systems Programmer Got Her Groove Back!

- The Problem?
- What is a Compensating Control?
- The Answer?
- Questions?
The Problem?

• z/OS requires a lot of “tweaking”
  • To take advantage of new function
  • To implement new versions of software
  • To make sure it keeps running

• Any change to z/OS could introduce problems
  • We use all the tools available to us to make sure they don’t
  • We religiously take backups
  • We are all trustworthy
  • We always think about security and compliance
  • Well maybe not so much…
What is a Compensating Control?

- A standard part of any security posture
- Must be based on risk analysis
- Legitimate technological/documentated business constraint
- Any compensating control must
  1. Meet the intent and rigor of the original requirement
  2. Provide a similar level of defence as the original requirement
  3. Be "above and beyond" other requirements
  4. Be commensurate with the additional risk imposed by not adhering to the requirement

- NOT a short cut to compliance!
The Answer?

• Use our experience

• Use IBM Health Checker for z/OS

• Use 3rd party tools
  • Image FOCUS
  • The Control Editor
  • StepOne
Image FOCUS

• Is very different from the IBM Health Checker for z/OS
  • Does a virtual IPL of your system
  • Will find problems in the whole chain
    • SYSn.IPLtparam
    • SYSn.PARMLIB etc
  • Keeps track of actual IPL volumes
  • Spots deficiencies in PARMLIB due to changed parameters between releases of z/OS
  • Can also track parmlib updates providing a simple back-out process for changes
  • Optional immediate email notification of problems found
Image FOCUS - Stories

- One of Our Variables Is Missing
- IPL Sleeper changes
- POR Sleeper changes
- New version of z/OS
- The Wandering Configuration
The Control Editor

• Risk Management Tool
• Enables Security to ALLOW vital changes
  • To the Technical Team that understands what is needed
  • Which Document and Verify:
    • What has ACTUALLY changed
    • Who ACTUALLY changed it and WHY
    • Optional email notification
  • Which satisfies Audit requirements
• Intercepts edit requests from TSO/ISPF
  • Customizable resources
  • Very reactive Development Team
The Control Editor - Stories

- We didn’t change anything...
- Late night shenanigans
- Do You Really Mean It?
StepOne

- Supplied for free
  - Written by Paul Robichaux CEO and Founder of NewEra Software Inc
- Creates a baseline for the whole System z Environment
  - Hardware configuration
    - OS config at IPL
    - POR values
    - Shared/shareable devices
  - IODF analysis
    - All LPARs
    - Not just those running z/OS
- www.newera.com/StepOne
z/Auditing Essentials Volume 1

- zEnterprise Hardware – An Introduction for Auditors
- Free
- Talks about System z security **BEFORE** RACF is active
  - Front Doors vs Back Doors
  - Not a new idea for Techies
  - Brand new to Audit!
- Hardware level security
  - Shareable I/O devices
  - HCD/HCM etc
  - Configuration Change Management
- Make sure any audit isn’t only valid on the day it’s performed
Questions?
Thank You

Julie-Ann Williams
Senior Technical Consultant
millennia…
julie@sysprog.co.uk
Session Number: 10103