

z/Auditing Essentials

Volume 1 – Front Doors

Agenda










- Mainframe Security
 - Past
 - Present
 - Future?
- Front Doors
 - What?
 - Where?
 - Specific examples to take away

Why should you care?

- Rumours of the death of the mainframe have been greatly exaggerated leading to...
 - Serious lack of investment in new personnel
 - Skilled personnel retiring
- Consequently...
 - No new Risk Analysis on System z in recent times
 - Security policies out of step with technology use
- New focus on audit means...
 - In depth analysis skills required
 - No centralised repository of knowledge

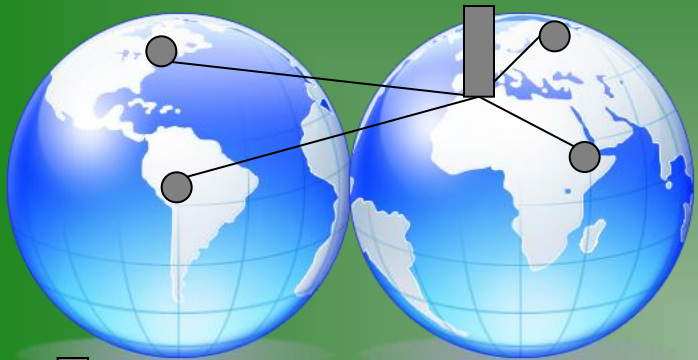
NewEra – Security Advisory Group

Council Members

-  NewEra
-  Mike Cairns
-  Brian Cummings
-  Dinesh Dattani
-  Stu Henderson
-  Martin Underwood
-  Craig Warren
-  Julie-Ann Williams
-  Mark Wilson



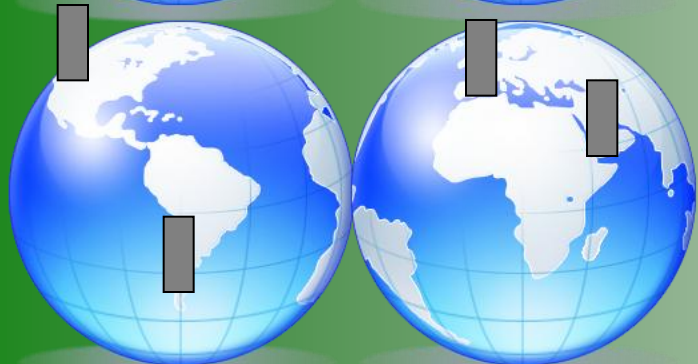
Growth Patterns in Business/IT



International (mid-19th to early 20th century)

Most operations are centred in the home country, with overseas sales and distribution.

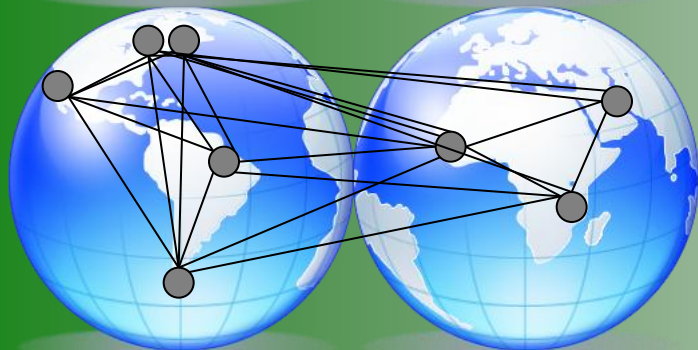
15 mainframes and growing



Multinational (mid-20th century)

Creates smaller versions of itself in countries around the world and makes heavy local investments.

1000s of mainframes and still growing



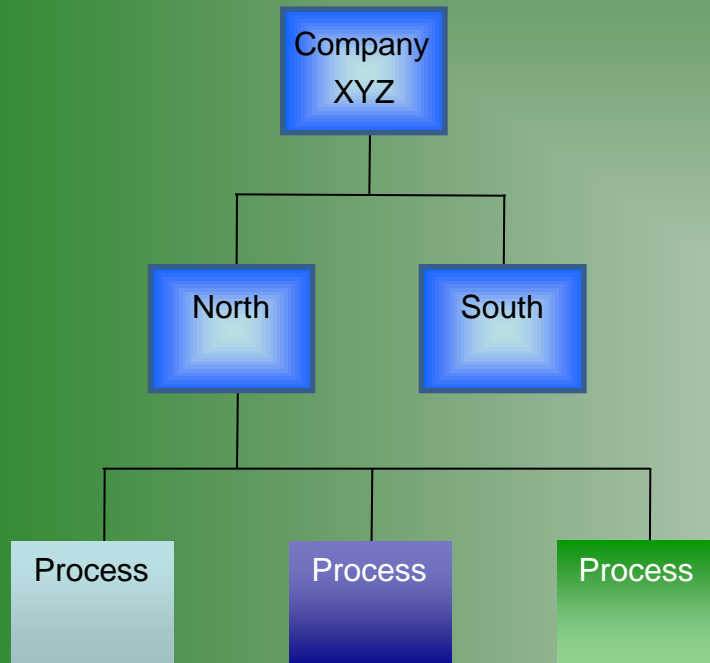
Globally Integrated Enterprise (21st century)

Locates operations and functions anywhere in the world based on the right cost, skills and business environment.

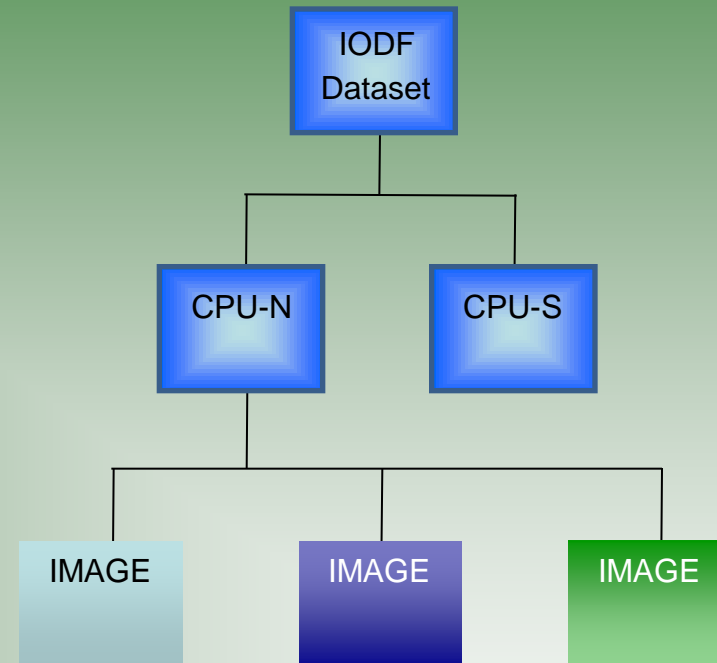
In excess of 10,000 mainframes and **still** growing

Business Structure vs z Implementation

Traditional view



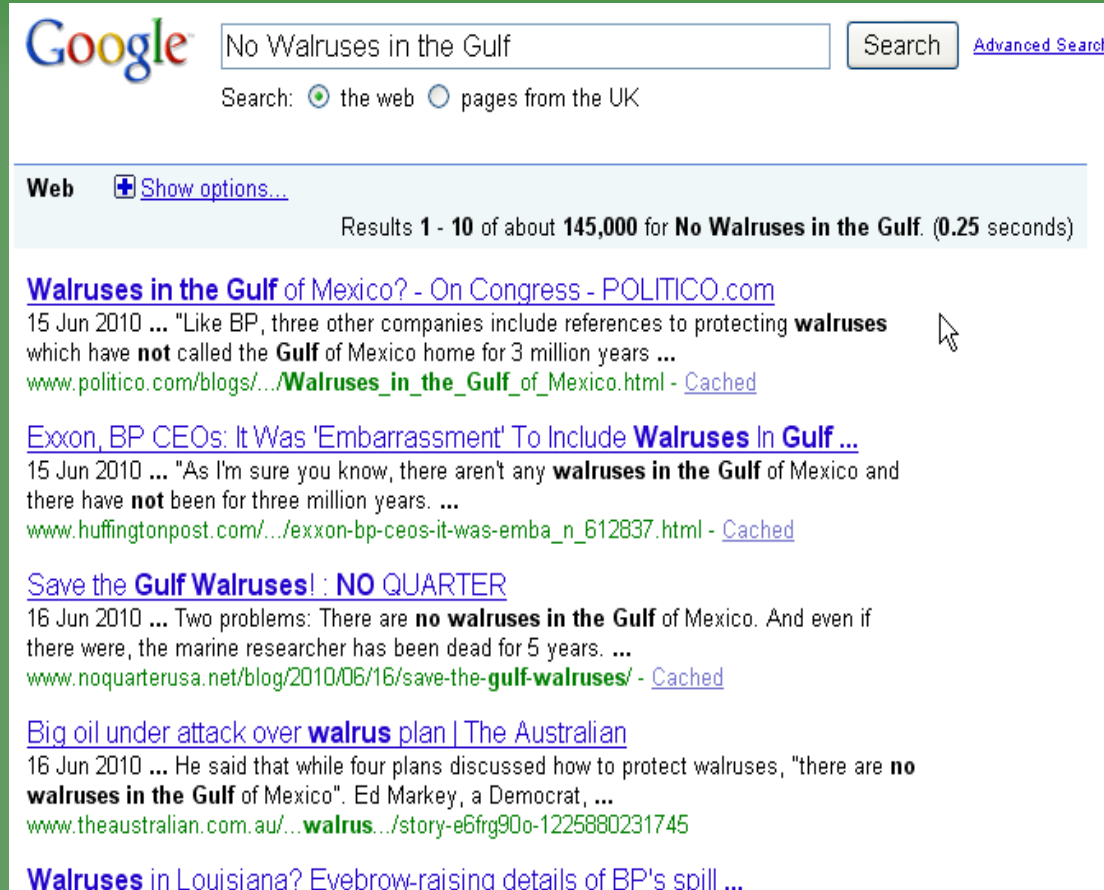
Business and Control Objects



z/Platform Control Objects

21st Century view is significantly different due to acquisitions etc

No Walruses in the Gulf!



The screenshot shows a Google search interface. The search bar contains the text "No Walruses in the Gulf". To the right of the search bar is a "Search" button and a link to "Advanced Search". Below the search bar, there are radio buttons for "the web" (selected) and "pages from the UK".

The search results are displayed under the heading "Web" with a "Show options..." link. The results show "Results 1 - 10 of about 145,000 for No Walruses in the Gulf. (0.25 seconds)".

The first result is titled "Walruses in the Gulf of Mexico? - On Congress - POLITICO.com" and dated "15 Jun 2010". The snippet reads: "Like BP, three other companies include references to protecting walruses which have **not** called the Gulf of Mexico home for 3 million years ...". The URL is "www.politico.com/blogs/.../Walruses_in_the_Gulf_of_Mexico.html - Cached".

The second result is titled "Exxon, BP CEOs: It Was 'Embarrassment' To Include Walruses In Gulf ..." and dated "15 Jun 2010". The snippet reads: "As I'm sure you know, there aren't any walruses in the Gulf of Mexico and there have **not** been for three million years. ...". The URL is "www.huffingtonpost.com/.../exxon-bp-ceos-it-was-emba_n_612837.html - Cached".

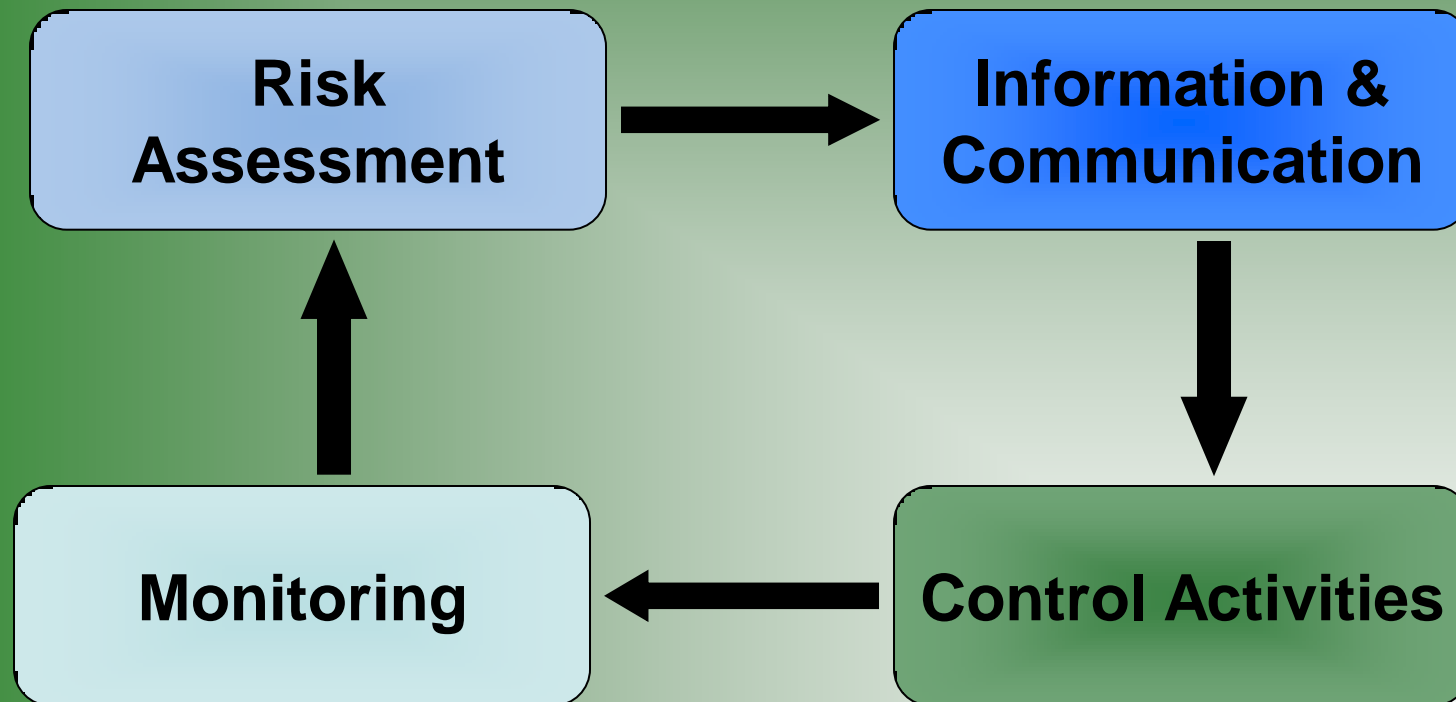
The third result is titled "Save the Gulf Walruses! : NO QUARTER" and dated "16 Jun 2010". The snippet reads: "Two problems: There are **no walruses in the Gulf** of Mexico. And even if there were, the marine researcher has been dead for 5 years. ...". The URL is "www.noquarterusa.net/blog/2010/06/16/save-the-gulf-walruses/ - Cached".

The fourth result is titled "Big oil under attack over walrus plan | The Australian" and dated "16 Jun 2010". The snippet reads: "He said that while four plans discussed how to protect walruses, 'there are **no walruses in the Gulf** of Mexico'. Ed Markey, a Democrat, ...". The URL is "www.theaustralian.com.au/.../walrus.../story-e6frg90o-1225880231745".

The fifth result is titled "Walruses in Louisiana? Eyebrow-raising details of BP's spill ...".

The very public result of not performing regular Risk Analysis

Internal Controls



Skipping any part of the process can cause unforeseen issues

What is a Front Door?

- Not BAU for Auditing System z!
- One can have flawless security systems on the Back Door but, if the Front Door is not at least closed, an opportunist thief can still take your belongings
- Partly physical & logical access to devices
- Partly securing APIs
- Partly managing configuration changes
- Front Door issues can lead to non compliance with SoX!

IODF

Functional equivalent of the PC BIOS

The Input/Output Definition File (IODF) is the set of logical configuration statements that are used to define a network of hardware resources. These resources are generally available to both the z/OS operating system (OSCP) and the z/OS platform hardware (IOCP) and related ESCON/FICON Directors (SWCP), if any.

Coupling Facility Risks

- Fundamentally no different to other PR/SM LPARs
 - Internal CF
 - IBM SoD suggests Dynamic Expansion for ICF will be dropped in the future
 - External CF
- Must secure CF Structures
 - e.g. LOGSTRM
 - SMF
 - OPERLOG
 - CICS

Operating System Risks

- Operating System configuration
- External Security Manager implementation
- I/O Device connectivity
 - Controlled by the IOCP
 - Part of the IODF
 - Arcane skill set
 - Rarely, if ever, audited
 - Access List
 - Candidate List

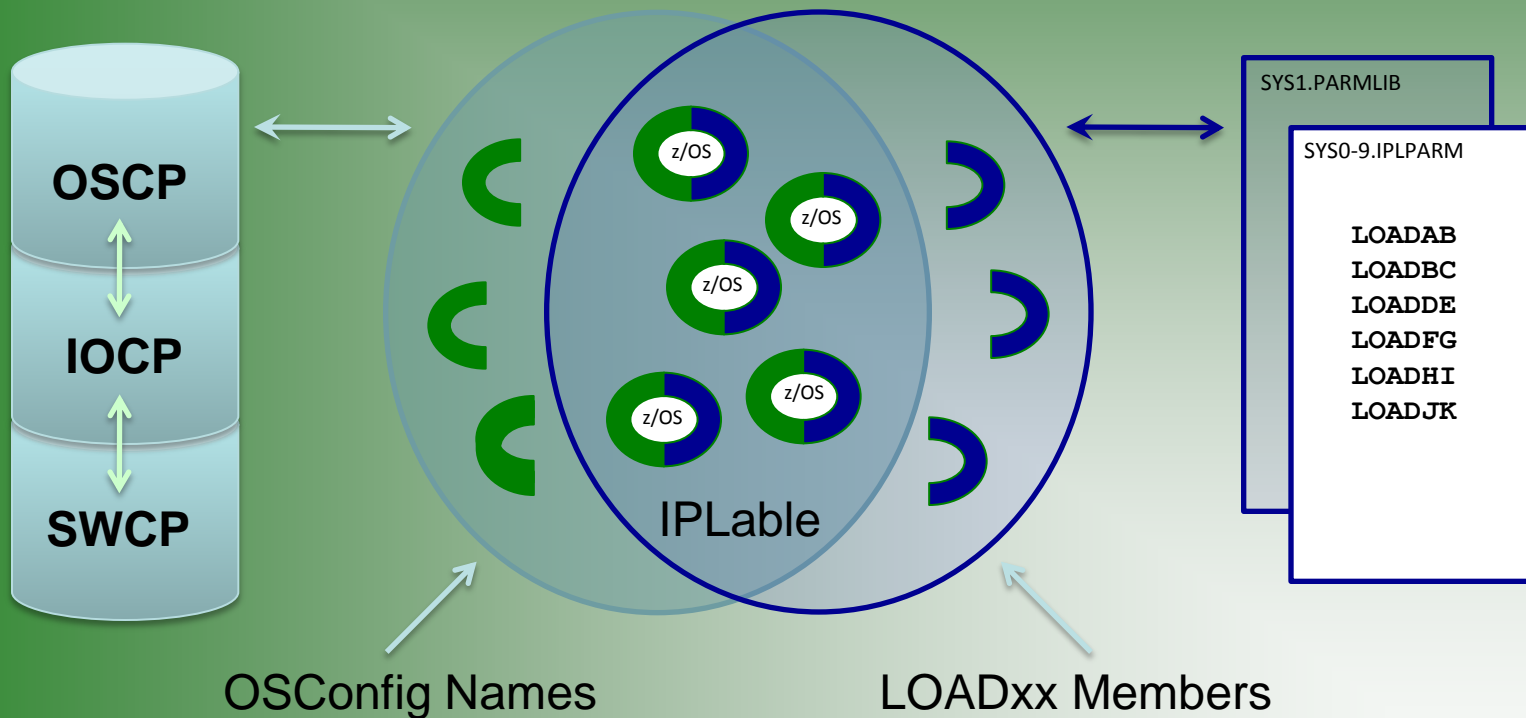
HCD/HCM/HMC

- HCD – ISPF dialog
- HCM – Workstation with GUI interface
- HMC – Optional GUI
 - Can be enabled to run remotely
 - Used legitimately to facilitate Automated Operations
- Combination approach
 - Physical security/CCTV
 - External Security Manager

NIP Consoles

- Nucleus Initialisation Process
 - IPL
- LOADxx
 - IODF
 - NUCLEUS
 - SYSPARM
 - NUCLST
- Never define a NIP Console in a public area!

Orphaned LOADxx Members



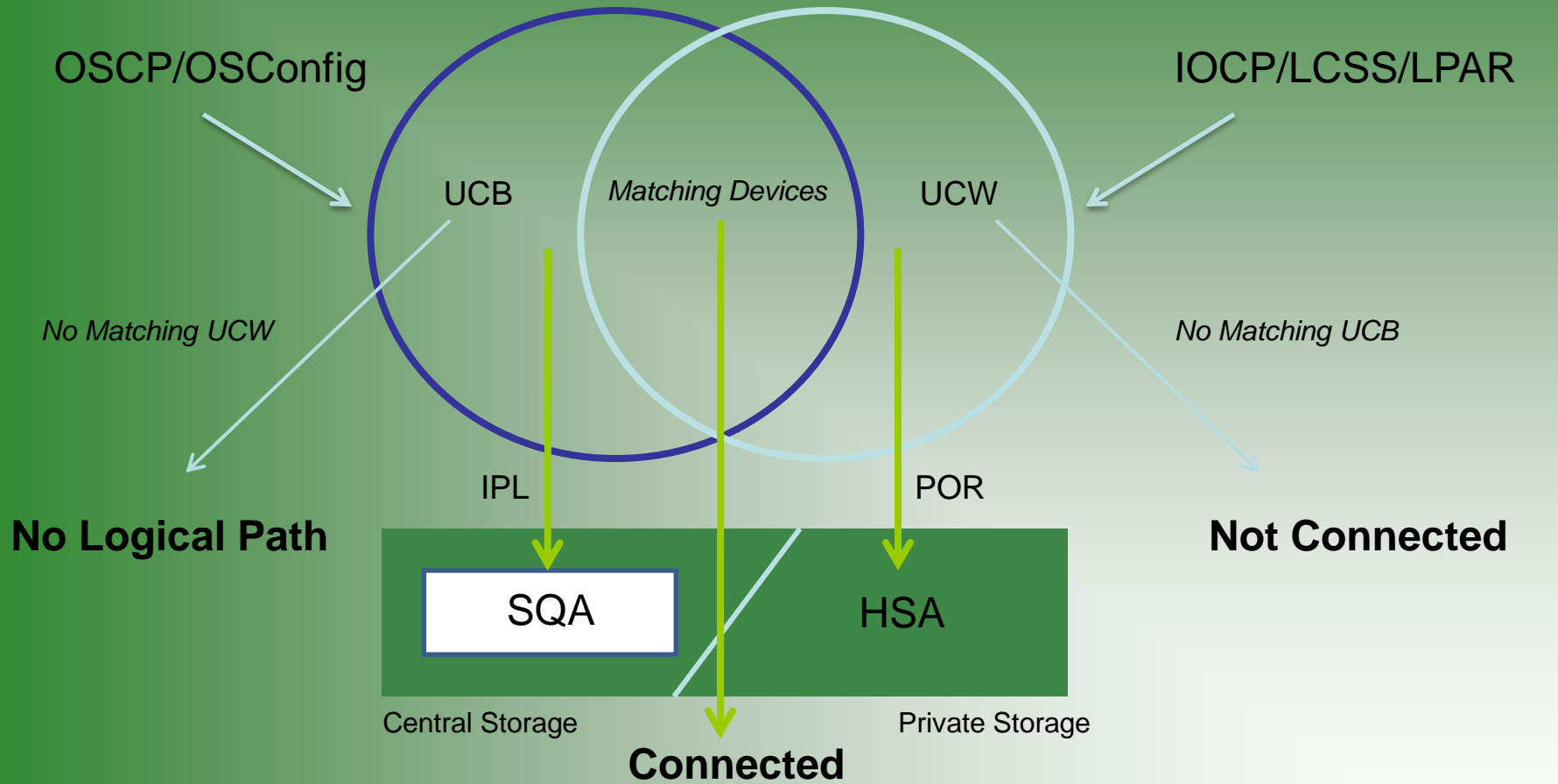
Can be used to "hide" IPLable systems

IMSI

- Initial Message Suppression
- Indicated by the last char in the LOADxx member
- Suppress messages
 - Doesn't lose data from log
 - Helps prevent msg overflow
- Suppress prompts
 - To prevent changes to OpSys
 - Use with care!
 - Can prevent recovery from system problems

IMSI Char	Display info Messages	Prompt for MCat Response	Prompt for System ParmS
A	Y	Y	Y
C	N	Y	N
D	Y	Y	N
M	Y	N	N
P	N	Y	Y
S	N	N	Y
T	Y	N	Y
. or Blank	N	N	N

Configuration Drift



SQA=System Queue Area

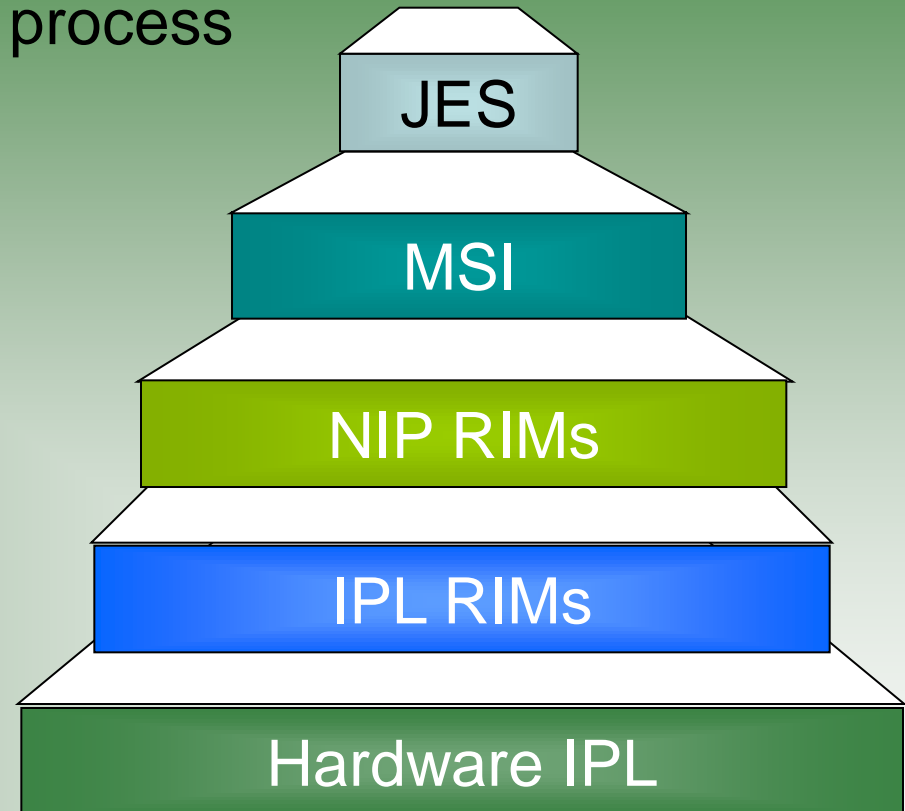
HSA=Hardware Storage Area

Dynamic Configuration Changes

- zEnterprise provides one of the most configurable hardware and operating systems combinations available
- Almost everything can be altered dynamically
 - To meet Business requirements on Demand
 - Can also be used to hack the system
- Over restricting use can cause operational issues
- Instead audit **ALL** activity
 - OPERCMDS
 - At least 34 critical dynamic change commands

IPL

- Functional equivalent of PC boot process
- Starts at the bottom
- Each step builds on the last
- No External Security Manager!
 - until late in the process
- Rarely audited
- Can be used to enable...
 - Real fixes for real issues
 - Front Doors to the system



System Integrity

- SHARE Security Project formed in 1972
- Mission:
 - Develop security requirements for future IBM Operating Systems
- Problem:
 - Any security could be bypassed if the defined Operating System Interfaces could be circumvented
- SHARE Security Project conclusion:
 - **There can be no System Security without Operating System Integrity**

System Integrity

- Problem not as prevalent as in the PC world
- 75+ Vulnerabilities on most z/OS systems!
- Can't be addressed with system settings or config
- Fixes available for most vulnerabilities
 - Security flagged APARs
 - Won't even know about the fix if you don't ask about the problem
- Vulnerability scans should be run on z/OS
 - Requirement for PCI, NIST 800-53, ISO 27001 etc
 - e.g. VAT (Vulnerability Analysis Tool)

Thank you for listening



My contact details in case you think of any questions after the event: julie@sysprog.co.uk

07770 415102