A Practical Approach to Zero Trust Architecture

Answering the requirements of NIST SP 800-27,
EU Commissions statement 22 March 2022
and the UK's NCSC 21 July 2021

ABSTRACT

Forrester Research has said “Zero Trust is becoming the security model of choice for enterprises and governments alike.”

If your CIO or CISO asked you to develop a ZTA plan for your mainframe, would you know where to start?

AGENDA

* Why is ZTA Important? What is ZTA?

* Zero Trust Architecture

* How to get started establishing a ZTA for IBM z/OS Systems

* An example of an actual exercise to create a ZTA for
  z/OS critical datasets

* A demonstration of The Control Editor (TCE)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

"Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows.

Zero trust "assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)."

– NIST SP 800-207
"Zero Trust Architecture"
August,, 2020

FORRESTER RESEARCH

"Zero Trust is becoming the security model of choice for enterprises and governments alike. However, security leaders often don't know where to begin to implement it, or they feel daunted by the fundamental shifts in strategy and architecture Zero Trust demands.

However, Zero Trust does not require that you rip out all your current security controls to start fresh, and with the right approach you can realize benefits right away."

– Forrester Research, Inc., report RES157736

WHAT ARE ZERO TRUST AND A ZTA?

Formal Definitions (from NIST SP 800-207)

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

MY DEFINITION

- A major de-emphasis on perimeter security.
- A terminal or a user is not trusted simply because he or she is inside the firewall or similar.
  - This is sometimes called “an assumed breach.”
- Protections of internal access just like external protections.
- A de-emphasis on trusted devices and trusted people.
- All security is transaction by transaction, or at least in some small window in time.
- Security is granular, it is not all or nothing.
- It is not that Bob is “trusted” – it is that he is authorized (or not) to do some particular transaction.
- This is sometimes called “least privilege.”

As you can see, a whole lot less trust …

WHO WANTS TO TELL THEM WE DON'T TRUST THEM ANYMORE?

THE GOAL FOR A ZTA IS TO RESOLVE 2 WEAKNESSES

First: Perimeter security is not enough

Second: USERs are Overprivileged

THE GOAL FOR A ZTA IS TO RESOLVE 2 WEAKNESSES

Perimeter security is not enough:

A ZTA should be designed to protect the important resources INSIDE the perimeter.
An Extra form of protection is needed once a user has gained access by ANY means.

Think of how you protect items in your life and home.

THE GOAL FOR A ZTA IS TO RESOLVE 2 WEAKNESSES

USERs are Overprivileged:

Example;
John is new to System support Group. His responsibility to review and update the Message suppression configuration. He will need access to the AO product and to the MPFLST00 member in PARMLIB. Since that member is in the PARMLIB dataset, he needs RACF granted access to the dataset. This would include ALL the members.

John is Overprivileged.
A ZTA must provide a method for John to do his job, and also protect access to the other members by John.

LOGICAL COMPONENTS OF ZTA

Policy Decision Point (PDP)

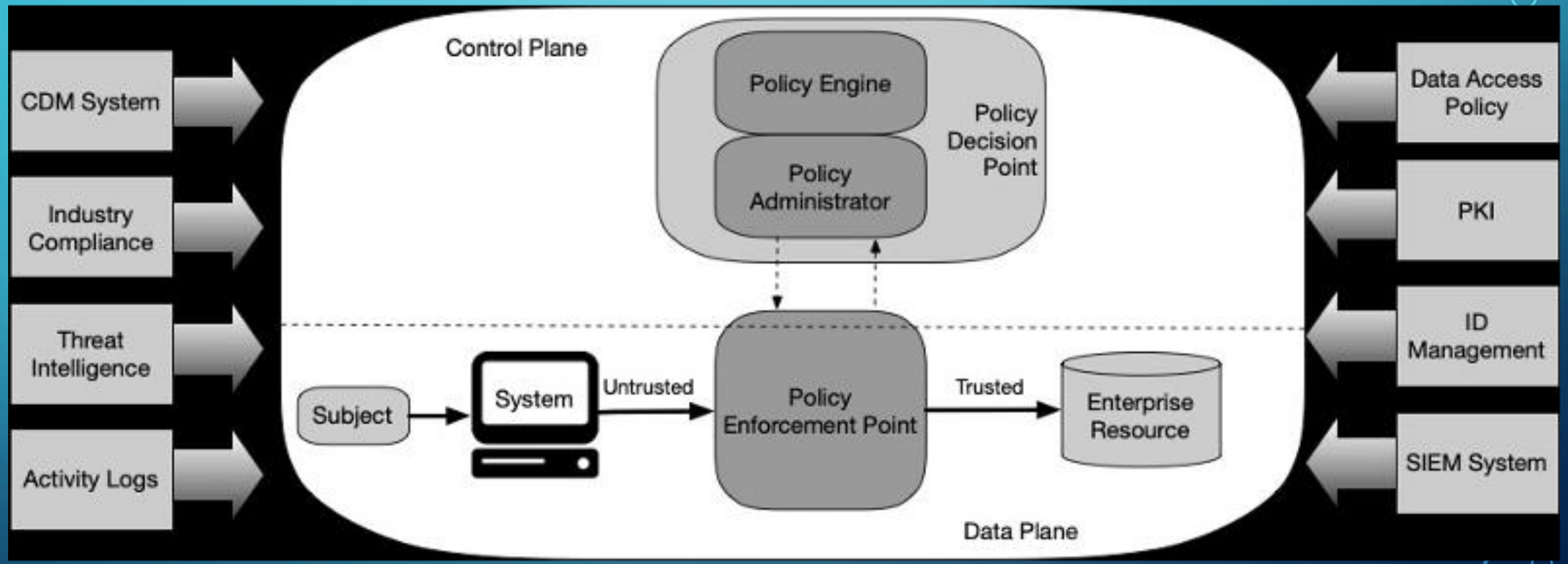
An organizational entity that orders the implementation, continuous review and the auditing of system controls.

Policy Enforcement Point (PEP)

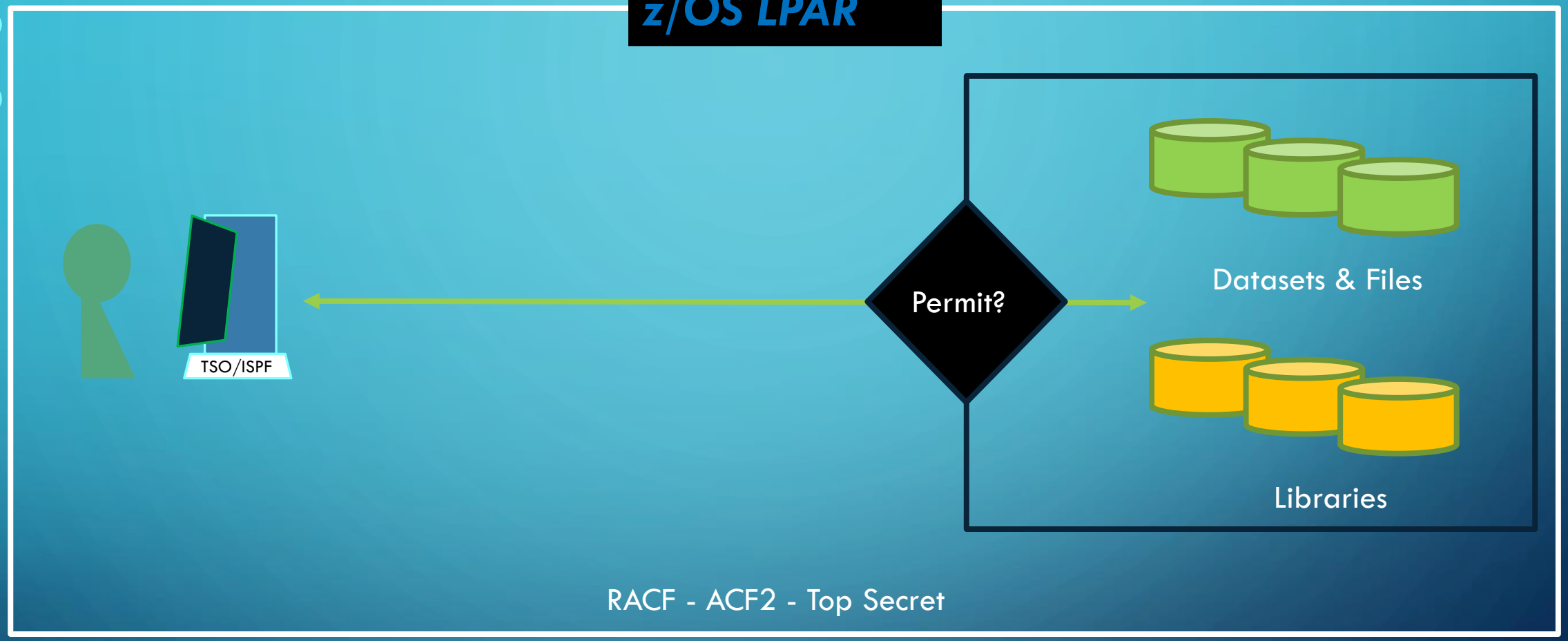
System entities that make ZTA authorization decisions for themselves or other system entities that request such services.

Extending the controls of: RACF, ACF2 and Top Secret - SAF

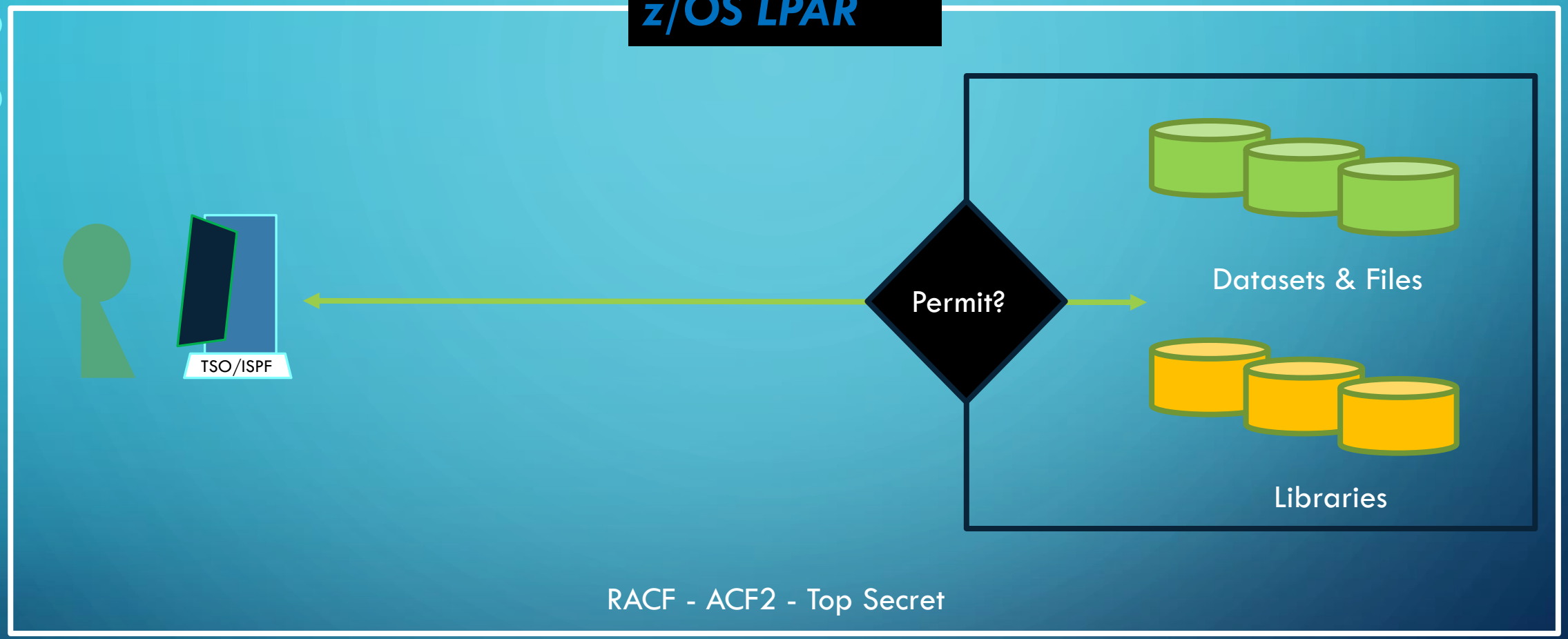
LOGICAL COMPONENTS OF ZTA



Perimeter Security



Perimeter Security



* Excessive access checking - The core part of protecting z/OS from malicious, hurtful activities. (ZTA)

*NIST - Dependency Mapping
SP 800-207 August 2020

NIST 800-53 AC AU CM IR

WOULD YOU KNOW WHERE TO START?

Pick a Target

APFLIST
LINKLIST
LPALIST
TCP/IP configuration files
PARMLIB
PROCLIB

WOULD YOU KNOW WHERE TO START?

Pick a Target

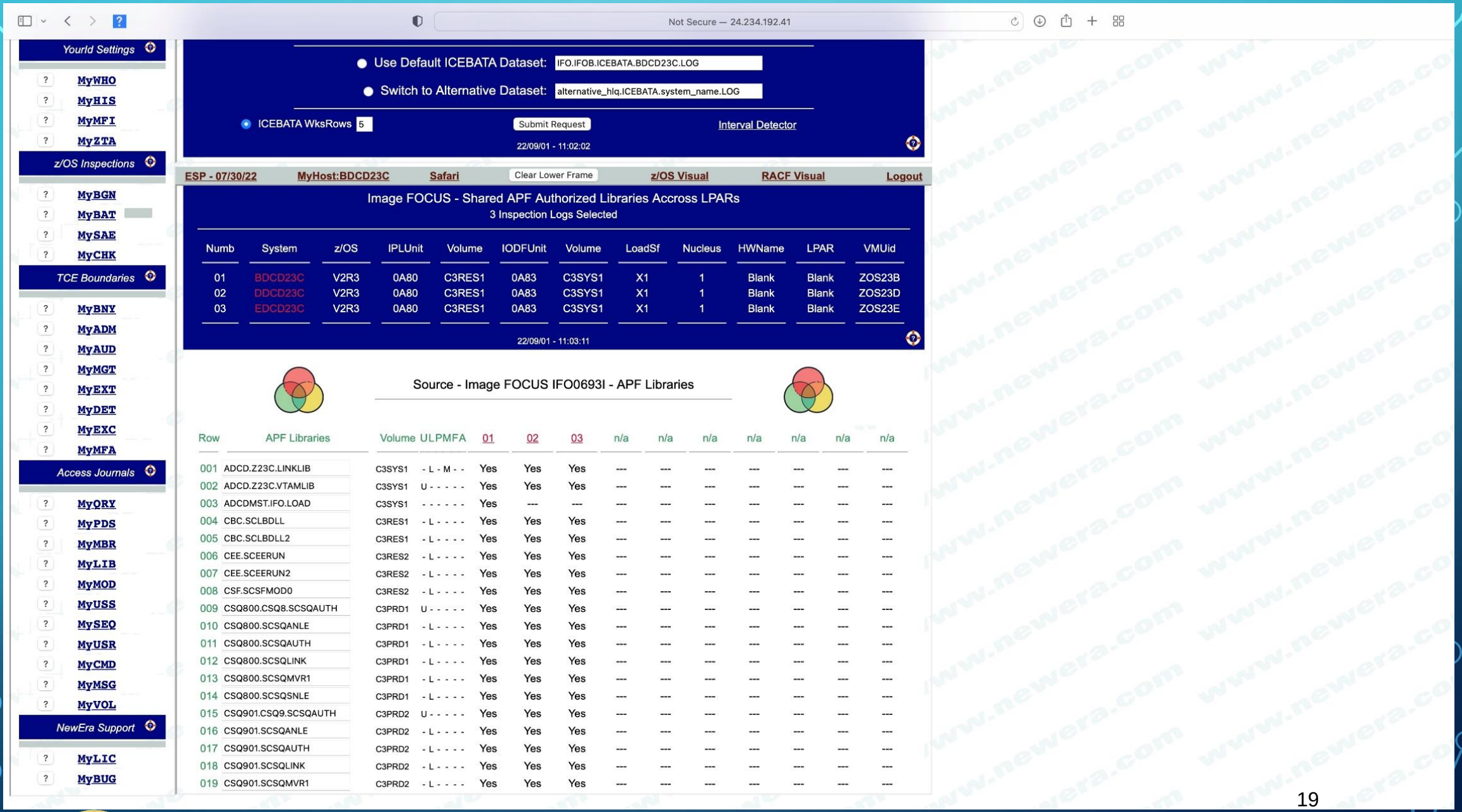
Take Inventory

WOULD YOU KNOW WHERE TO START?

Pick a Target

Take Inventory

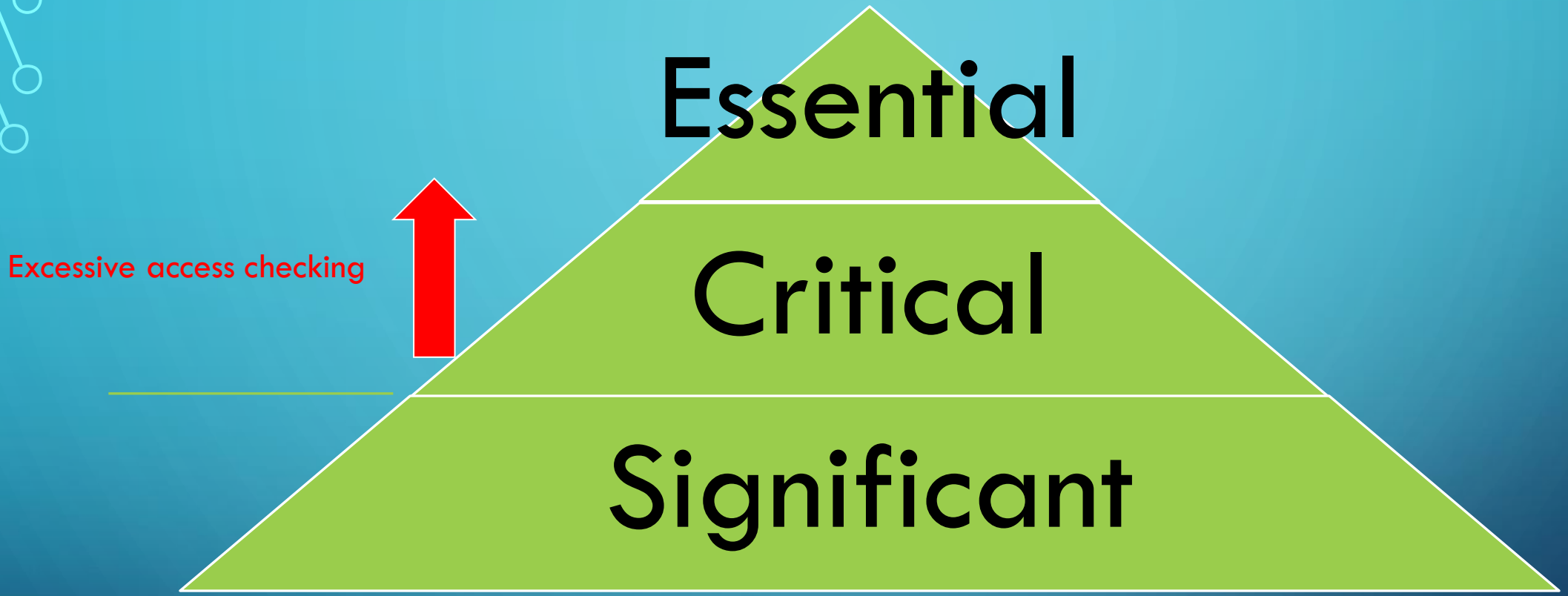
Evaluate the Importance of the Resources


Not Secure — 24.234.192.41
YourId Settings
MyWHO
MyHIS
MyMFI
MyZTA
z/OS Inspections
MyBGN
MyBAT
MySAE
MyCHK
TCE Boundaries
MyBNY
MyADM
MyAUD
MyMGT
MyEXT
MyDET
MyEXC
MyMFA
Access Journals
MyQRY
MyPDS
MyMBR
MyLIB
MyMOD
MyUSS
MySEQ
MyUSR
MyCMD
MyMSG
MyVOL
NewEra Support
MyLIC
MyBUG
Use Default ICEBATA Dataset: IFO.IFOB.ICEBATA.BDCD23C.LOG
Switch to Alternative Dataset: alternative_hlq.ICEBATA.system_name.LOG
ICEBATA WksRows 5
Submit Request
Interval Detector
22/09/01 - 11:02:02
ESP - 07/30/22
MyHost:BDCD23C
Safari
Clear Lower Frame
z/OS Visual
RACF Visual
Logout
Image FOCUS - Shared APF Authorized Libraries Accross LPARs
3 Inspection Logs Selected
Numb System z/OS IPLUnit Volume IODFUnit Volume LoadSf Nucleus HWName LPAR VMUid
01 BDCD23C V2R3 0A80 C3RES1 0A83 C3SYS1 X1 1 Blank Blank ZOS23B
02 DDCD23C V2R3 0A80 C3RES1 0A83 C3SYS1 X1 1 Blank Blank ZOS23D
03 EDCD23C V2R3 0A80 C3RES1 0A83 C3SYS1 X1 1 Blank Blank ZOS23E
22/09/01 - 11:03:11
Source - Image FOCUS IFO0693I - APF Libraries
Row APF Libraries Volume ULPMFA 01 02 03 n/a n/a n/a n/a n/a n/a n/a
001 ADCD.Z23C.LINKLIB C3SYS1 - L - M - - Yes Yes Yes --- --- --- --- --- --- ---
002 ADCD.Z23C.VTAMLIB C3SYS1 U - - - - - Yes Yes Yes --- --- --- --- --- --- ---
003 ADCDMST.IFO.LOAD C3SYS1 - - - - - - Yes --- --- --- --- --- --- --- --- ---
004 CBC.SCLBDLL C3RES1 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
005 CBC.SCLBDLL2 C3RES1 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
006 CEE.SCEERUN C3RES2 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
007 CEE.SCEERUN2 C3RES2 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
008 CSF.SCSFMOD0 C3RES2 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
009 CSQ800.CSQ8.SCSQAUTH C3PRD1 U - - - - - Yes Yes Yes --- --- --- --- --- --- ---
010 CSQ800.SCSQANLE C3PRD1 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
011 CSQ800.SCSQAUTH C3PRD1 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
012 CSQ800.SCSQLINK C3PRD1 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
013 CSQ800.SCSQMVR1 C3PRD1 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
014 CSQ800.SCSQSNLE C3PRD1 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
015 CSQ901.CSQ9.SCSQAUTH C3PRD2 U - - - - - Yes Yes Yes --- --- --- --- --- --- ---
016 CSQ901.SCSQANLE C3PRD2 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
017 CSQ901.SCSQAUTH C3PRD2 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
018 CSQ901.SCSQLINK C3PRD2 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---
019 CSQ901.SCSQMVR1 C3PRD2 - L - - - - Yes Yes Yes --- --- --- --- --- --- ---

WOULD YOU KNOW WHERE TO START?

- The APF LIST example has a variety of DATASETS;
  - 20 different HLQs Almost 200 datasets
    - 13 start with SYS1
    - 5 start with TCPIP
  - How do you understand the role and importance of each category of dataset?
  - How do you understand what controls should be on each category of dataset?

WOULD YOU KNOW WHERE TO START?



ALL of the DATASETS are Important

START WITH THE CONTROL EDITOR (TCE)

- Capabilities for PDPs and PEPs:
  - 1. Backup prior to any change
  - 2. Detected changes
  - 3. Documentation of change
  - 4. Notification of change via email or SMS
  - 5. BATCH changes must be supported
  - 6. Additional PASSWORD required
  - 7. ACCESS determined at the MEMBER level
  - 8. ACCESS granted by type of request
  - 9. Additional TOKEN challenge

Excessive access checking

START WITH THE CONTROL EDITOR (TCE)

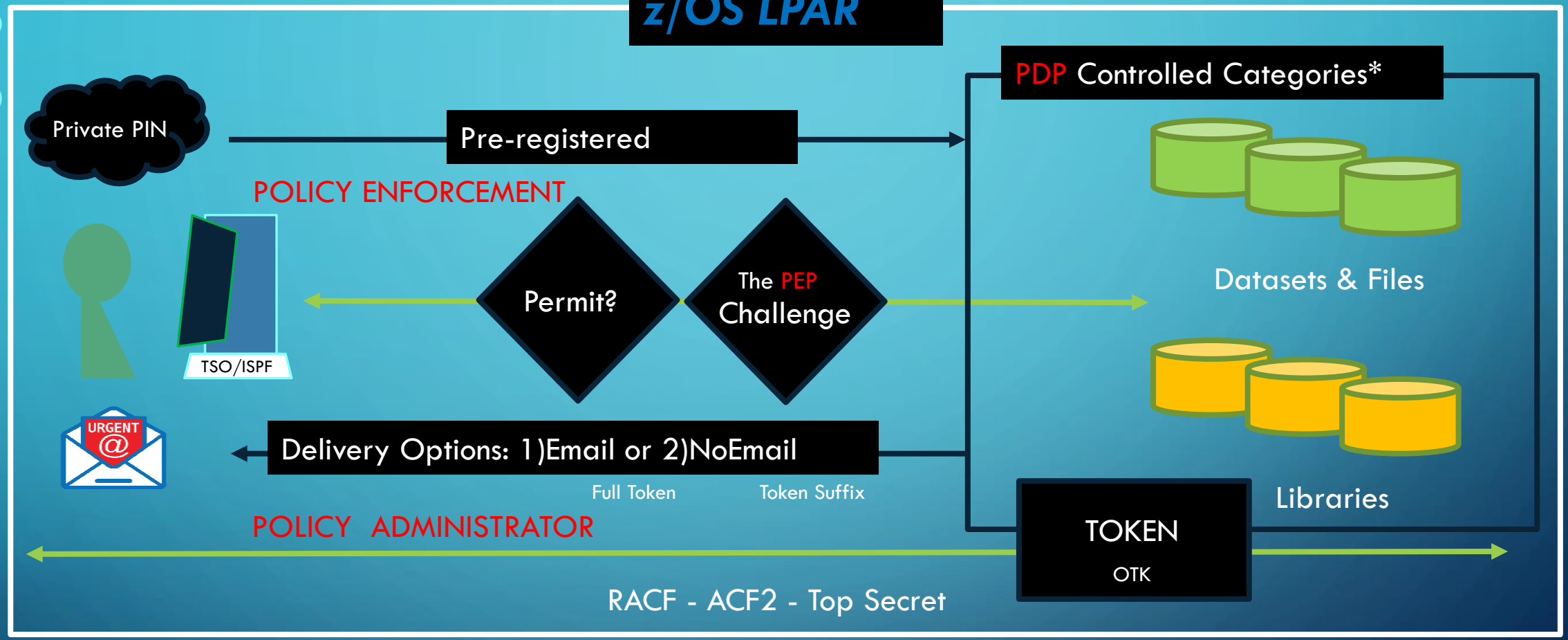
Map to TCE Capabilities

ALL of the DATASETS are Important

Policy Enforcement Point Policy Decision Point TCE

z/OS LPAR

POLICY ENGINE



* Excessive access checking - The core part of protecting z/OS from malicious, hurtful activities. (ZTA)

Controlled Categories and Journals

*NIST - Dependency Mapping
SP 800-207 August 2020

NIST 800-53 AC AU CM IR

THE GOAL FOR A ZTA IS TO RESOLVE 2 WEAKNESSES

First: Perimeter security is not enough

Second: USERs are Overprivileged

The Control Editor from NewEra Software provides the ability to overcome these weaknesses

A PRACTICAL APPROACH TO ZERO TRUST ARCHITECTURE

Thank you for attending and if you have any questions
or if you would like more information please contact me.

Glennon Bagsby
GHB@NEWERA.COM
WWW.NEWERA.COM