INTEGRITY CONTROLS ENVIRONMENT

The Four Pillars of z/OS Operational Integrity

Integrity Controls Environment (ICE) from NewEra Software, Inc. helps you create and maintain a highly available, safer and more secure IT environment for your business applications, based on its ability to:

1. Maintain and increase the availability of z/OS and therefore the access to applications that run on the mainframe;
2. Lower the cost of providing z/OS services and administration protocols while automating change management and impact review, enforcing enterprise standardization and reducing risk;
3. Extend security and controls beyond those provided by legacy security managers such as RACF, CA ACF2 or CA TSS. Reduce manual exposures in change management and increase real-time audit on administrative events.
4. Critical real-time notification of any activity that may prove to be a risk to your system's integrity without the delay of other solutions that require processing of large amounts of data or after the fact analysis.

MAINTAIN AND INCREASE z/OS AVAILABILITY

High availability is one of the cornerstones of the IBM mainframe and z operating system. For over 25 years, NewEra Software has helped its customers maintain high availability standards and, as confirmed by users globally, actually increase availability by providing the tools to help monitor, test and report on the integrity of the z/OS system configuration.

Image FOCUS (IFO), an integral part of the Integrity Controls Environment, has a unique and powerful capability that performs an Inspection of the configuration files needed for z/OS to initialize, or IPL. This inspection identifies any problems or risk that may exist within the definitions stored in the PARMLIB members and start up procedures for the operating system and sub-systems.

Users can run an Inspection on demand, on a user-defined interval, in Batch, or as part of the monitoring provided by the IBM Health Checker for z/OS.

In addition to analysis for existing problems and risks, the inspection process can also detect and report changes made to an IPL structure, including changes made dynamically by use of operator commands. Taking this process a step further, it confirms dynamic changes which should be permanent within the relevant PARMLIB members or need to be reapplied after new IPL.

With this unique software product, you can monitor your z/OS systems automatically and be made aware of any changes made to critical configuration files; ensure those changes will not have a detrimental effect on availability of your systems and therefore business applications; and your system is secured to the standard you must establish as required by IBM and auditors.

Any problems, risks, or exposures are detected and notices sent before there is a loss of service or delay in starting an LPAR or adding new service to an existing LPAR or Sysplex. With the implementation of ICE products, improvements and changes are tracked, reported, tested and an audit trail created automatically.

This creates an environment where there are fewer instances that could delay the availability of the entire z/OS platform to your customers and users. The testing and certification process, with automated change and impact documentation, also shortens the time needed to make improvements and repairs. It ensures that those actions are done correctly on first change request, thereby preventing delivery delays and increasing availability.

Optional applications extend the Inspection Process to:

- JES2/3
- VTAM
- TCP/IP
- CICS
- IODF
- RACF
- Load Libraries
- Modules
- OMVS
- PPT
- More…

LOWER THE COST OF PROVIDING z/OS SERVICES

A 2016 Ponemon Institute survey reported the average cost of data center downtime had increased to $531,060 per hour. This figure grows based on the size of your business.

The need for high availability leads to the subject of risk and cost. We can all agree that if the business applications that run on z/OS are not available, the organization and business will suffer. The ICE products can greatly reduce the risk of having an extended outage, thus removing this as an issue and incurring the huge cost of downtime and follow-up reviews and audits.

When something as simple as a misplaced comma or keyword with a bad value can stop an IPL, it is better to find and correct those problems before an IPL is attempted. Image FOCUS can detect those problems and many more complex issues, so that you can prevent undetected problems from becoming a major issue by delaying the IPL and the startup of your business applications.

While eliminating downtime provides significant cost savings, increasing systems professionals' productivity can also provide real cost savings to the organization. One example is the project of upgrading the release level of z/OS. The amount of time needed to research changes needed to upgrade, make and test changes, document the work and finally rollout the upgrade across the enterprise can take several months.

Users who employ our New Release Analysis (NRA) tool confirm they have reduced that time by several weeks in each phase of the upgrade process. New Release Analysis identifies exactly what changes are needed to your existing system to successfully perform the upgrade. NRA tests each change as it is encountered and verifies that it will be correct for the new release.

With another ICE product feature, The Controls Environment (TCE), each change is automatically recorded, documented, tested and team members (and management systems) are notified of the completion of that task. Automating day-to-day tasks provides yet another opportunity to realize significant cost savings. A simple edit may require that first a backup be taken before the change is made, the change needs to be documented and include back out instructions; it must be tested and notification must be made to anyone else who has a need to know about the change.

With TCE these tasks can be automated and fully integrated so the software performs the backup, provides the template for change management processes, tests the change (impact in member, image and sysplex) and sends notification on the exact change executed by each administrator each time one is made. Having TCE take on these tasks means you can use it to establish and control policy standards and best practices that are consistent and followed by all – in-house staff and external consultants.

The productivity gains are significant and many projects are completed ahead of schedule, without problems, cutting weeks off your project plans. Auditors and Management have legible reports tied in with assigned change events - you see in text format the exact changes implemented during a change request and impact of that change. What would this be worth to your organization?

Then consider the veiled cost of reversing a task that has been performed without following policy standards – whether by accident or on purpose. Something as simple as not creating a backup prior to a change or not providing documentation can not only potentially mean loss of availability but may lead to hours of extra time spent in order to determine the problem and provide corrective action.

So yes, the Integrity Controls Environment can help reduce the risk of a major outage, but can also reduce the cost to deliver enhancements and changes by system administrators. It provides great benefit on a daily basis to the system professionals that are monitoring and maintaining the z/OS system and your business applications.

EXTEND SECURITY AND CONTROLS BEYOND WHAT'S PROVIDED BY THE ESM.

TCE can improve and strengthen access rights…

Equally important in any discussion about availability and lowering the cost of providing service must include extending security. A loss of any kind due to poor security will affect availability and raise the cost of providing reinstatement services.

Regardless of which security manager you have in place, the ICE products extend the protection provided for your most critical datasets and libraries by your External Security Manager (ESM). This is done in several ways including improving access rights, enforcement of policies, and providing audit trails for all activity that could affect the integrity of the z/OS environment and your business applications.

TCE improves access rights by allowing for the TCE administrator to easily establish permission rights at the "member level" of a PDS/PDSE control dataset. This provides for refinement of access to a specific user or group of users to only those members that are needed by those users in performance of their duties, regardless of the dataset level access rights granted by the ESM.

All attempts to access those members, successful or not, are recorded in a journaling system and notification emails can be sent automatically to managers and management systems. If changes are made to a member, a new backup of the member is created automatically, enforcing the policy that a backup must be taken prior to a change being made to a member or dataset.

TCE can improve and strengthen access rights by establishing a second level of authorization for access. An additional password must be provided to access a dataset or a group of datasets. This powerful and unique feature of TCE allows for protection to the most important datasets that are seldom changed except in time of emergency. This second password procedure can be set by an administrator and changed dynamically when needed.

TCE can enforce other policies and controls by establishing a level of documentation through the use of descriptor panels, which require site-specific information be entered for each action taken by a user. With TCE it is possible to present to the user, at the time that the action is being taken, a predefined form that must be fully completed at that moment before the action can proceed (e.g. Edit, Operator Commands…). This will provide a standard for documentation that must be followed and create an audit record for this action that becomes part of the history of activity for that resource and user.

This documentation can be a source of information to be provided to other applications such as SIEM products and change management services.

Controls can be created and policies established for activities such as Edit functions, Submit, Delete and Rename. Similar controls can be used for batch processes when that is the method used to alter these critical z/OS datasets. TCE can also record the use of commands and, with the addition of the OPER option, can control access to commands with passwords, require the use of descriptors for documentation, and log ALL commands into a separate log that is easily accessed.

The ICE facilities also have the ability to inspect the RACF SETROPTS configuration on all LPARS with a Health Check, under the control of the IBM Health Checker for z/OS, or as a Detector with the ICE application. This inspection is performed using site-specific rules and requirements to create a repeatable method for self-auditing of the RACF critical settings. This check also will monitor those settings for changes and will provide detailed reports of changes, as well as other issues discovered during the inspection.

REAL TIME NOTIFICATION OF USER ACTIVITY THAT CAN IMPACT Z/OS INTEGRITY

ICE/PSWD provides notification of use at logon…

NewEra continues to provide innovative new products and capabilities that address the changing needs of maintaining Operational Integrity. One of the most critical factors in providing that integrity is the people and staff that support the z/OS systems. It is then most important that we include those people in the defense perimeter of these systems. A very simple idea - that only the user who takes some action knows if that action was indeed performed by him or her.

If we are concerned about who has accessed our system by logging onto TSO, CICS, FTP and/or others, wouldn't it be vigilant to ask the person who logged on, "Was that you or was it someone else who may have used your credentials?"

With the increased concern over, and frequency of HACKING and malicious events, a new requirement has arisen for faster awareness of these events. This is true for both successful and unsuccessful events. Waiting for days, or weeks, before a HACK attempt is identified by processing historical records is no longer acceptable. The longer the period of time passes between these events, their detection and corrective action is taken greatly increases the risk to an organization, its productivity and its business reputation.

The newest of the ICE facilities, ICE/PSWD, addresses this by providing real time notification to users, supervisors, and risk managers of any activity that could impact z/OS available.

This includes logon activity of privileged users, failed login attempts, PASSWORD changes, edits of critical datasets, operator commands and unusual behavior or activity at unexpected times.

We have become accustomed to these types of notifications and awareness from our social media and internet accounts; what NewEra has done is provided the same to the z/OS platform.

ICE/PSWD

ICE/PSWD provides notification of credential use, at logon, gives your users confidence that their integrity and the integrity of the system has not been undermined by credential theft. Notification of password/phrase reset request/ attempt provides users additional assurance that overall integrity remains intact and that they have not been 'Locked Out'.

At login and at PASSWORD/ PASSPHRASE reset, ICE/PSWD provides an effective and efficient all software solution to Multi-Factor controls. For logon, ICE/PSWD employs the best MFA concepts, i.e., the user never knows the complete password/passphrase in advance of the logon request, while at the same time preserving the user's RACF credentials and RACF's ultimate control over the user logon.

For PASSWORD/ PASSPHRASE reset, the user is provided a One-Time Password (OTP) suffix, to which they append their secret prefix, and return to complete the reset.

Additional PASSWORD/ PASSPHASE services are provided in the form of enhanced expiration notices, and binding USERID to PASSWORD format rules defined by RACF.

ICE/PSWD also provides alerts of failed logon attempts, either by invalid USERIDs or failed PASSWORD/PASSPHRASES. These alerts are sent in real time via email or text and can be activated or deactivated by day, time, userid, or type of event. Reports of activity can also be generated and sent to individuals via email or text and can also be routed directly to a SIEM, and the ICE journaling system.

Integrity Controls Environment (ICE) Products

IFO provides the capability to perform inspections of an IPL structure and determine if there are any risks…

Image FOCUS (ICE/IFO)

IFO is one of two foundation products for ICE. IFO provides the capability to perform inspections of an IPL structure and determine if there are any risks, problems or points of failure within the use of the configuration datasets and members for any version of z/OS. This inspection can be performed for an entire SYSPLEX, an individual LPAR, or a named member. This inspection can be executed online, in batch, or automatically on a preset schedule.

IFO can also monitor those configurations to identify changes made to the datasets and can provide an automated method of sending alerts when a problem or a change is detected. Additionally, IFO can make backups of the configuration whenever changes are made, creating audit and recovery points automatically.

IFO also provides integrated testing and simulation functions, such as simulating release level changes, or testing planned changes with the use of a temporary or staged parmlib dataset.

IFO also can provide a unique Recovery capability that will allow access to ISPF without the requirement of JES, VTAM, or TSO.

IFO also provides additional change detectors that monitor other vital areas of z/OS that are not a part of the IPL process directly. These detectors will monitor for changes to such things as RACF, SVC's, IODF, the OMVS system profile, and many more. Each detector will build a baseline and perform a comparison on a scheduled interval, or on demand, and will send email notifications when changes have been detected.

Optional IFO Applications

Subsystem Inspectors (ICE/SUBS)

The Subsystem Inspectors add the ability to simultaneously inspect critical systems, perform full inspections for JES 2/3, VTAM, TCP/IP, CICS, RESOLVER, TELNET, OMPROUTE, and more. The Inspectors perform the same level of analysis and will track changes in the same way that the base IFO product manages the Operating System.

Supplemental Inspectors (ICE/SUPS)

The Supplemental Inspectors extend the inspection process to include Load libraries and datasets not included in the IPL process. The inspection of load modules named to the Supplemental Inspectors will identify critical problems such as orphaned aliases or duplicate modules in an operational list such as the LPALST.

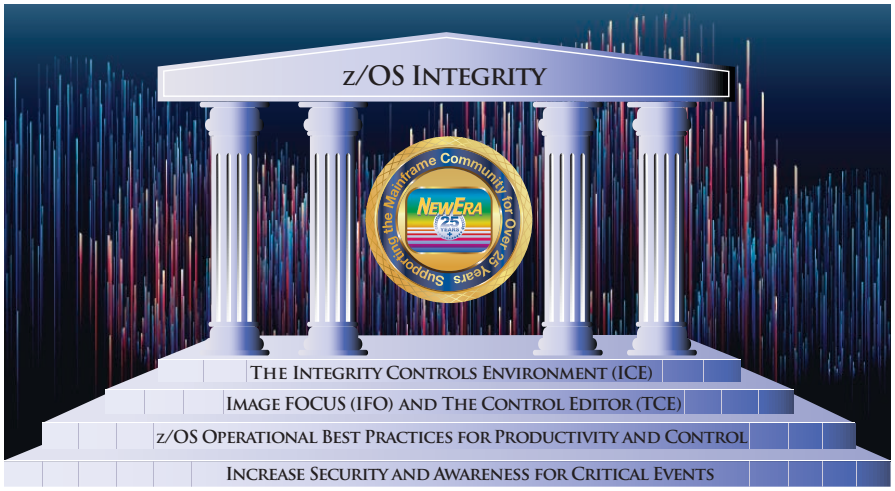
The Controls Environment (ICE/TCE)

TCE is a next generation change management tool that provides not only automation for tasks often associated with change activity but also extends the controls and security of legacy ESM products, such as RACF, CA ACF2, or CA Top Secret. TCE will monitor and participate in the change process of named, essential datasets. TCE will automate the creation of backups and send notifications of all activity. This activity includes EDIT functions, SUBMIT, and the use of operator commands.

All change information captured by TCE is written into a journaling system to provide audit and recovery information. The change information captured at the time of any activity can be supported by the use of an interactive descriptor process which can be set up to require the user to document the activity in a standard form designed by the administrator for policy enforcement. This additional documentation becomes a permanent part of the activity record in the journal.

The Email notification, SIEM interface and the ability to update CLOUD based reporting systems can provide the immediate reporting of activity detected by TCE.

TCE also has the capability to establish additional access rights to datasets and members that exceed those provided by installed ESM. These additional



rights include member level access rights, which allow for refinement of access to members in shared datasets. TCE can also be used to establish a second level of authorization at the dataset level by means of requiring a second password for access.

Included with IFO and TCE is a powerful capability to track and record the use of operator or ESM commands. We know that dynamic changes are made to the running system and the ESM control are updated via commands, but the use of those commands can be difficult to audit and do not provide an immediate notification of the action taken with the issuance of those commands. With addition of the command logging facility introduced in Release 12 of ICE we can provide an easy method of command tracking, auditing and full transparence of dynamic changes made with commands. This logging can be further enhanced with the inclusion of the OPER optional products.

Optional TCE Applications

OPER/MVS

OPER/MVS provides capabilities in parallel to TCE by adding additional control and security over operator commands. In addition to having the command activity recorded in the TCE journals, OPER/MVS will create a log of ALL commands separate from the SYSLOG so that command activity is more transparent and easily audited. OPER/MVS can also provide access security to commands and enforce the use of descriptors for documentation. Email notification, SEIM interface and the updating of CLOUD based reporting when commands are used is also provided by the OPER products.

OPER/RACF

OPER/RACF is similar to OPER/MVS with the exception that it provides the same capabilities for the use of RACF commands. This is critical for RACF change activity, audits and problem resolution.

IPLCHECK – Works in Conjunction with the IBM Health Checker for z/OS

IPLCheck CORE is a repurposing of the inspection process from ICE/IFO. This check will automatically determine the IPL structure used to start the LPAR on which it is active and will inspect that structure to determine the integrity of the process so if a new IPL is attempted, it would be successful.

This same inspection can be performed for non-running LPARs with **IPLCheck ALT** and for any JES subsystem with **IPLCheck Subsystem**.

IPLCheck Dynamic determines if the content of certain PARMLIB members processed at a future IPL will match the current values of the active system, including System Symbols, APFLST, LPALST, LNKLST and the BPXPRM definitions.

IPLCheck SETR inspects ALL the options defining the core settings of RACF. The rules can be defined by the user or the default rule set; DISA standards can also be used. This provides for self-auditing your RACF standards with each execution of the check. It also provides change detection of the RACF configuration options.

NewEra Software, Inc.
Morgan Hill, CA 95037
800-421-5035
www.newera.com
support@newera.com

NewEra is the proud sponsor of The z Exchange. The z Exchange is a worldwide virtual User Group dedicated to providing and exchanging information that helps practitioners in the z Community better deliver service to their organizations.

Visit https://zexchange.info for more information on the current slate of webcasts. A link on that page will take you to our monthly Calendar of Events so you can register for the webcasts of your choice.