The Control Editor, operating within or outside the z/OS Integrity Controls Environment (ICE), detects, records and reports on events that change z/OS LPAR configurations.

The Control Editor

15.0

Getting Started

Contact us for additional information:

NewEra Software Technical Support

800-421-5035 or 408-201-7000
Or text support requests to 669-888-5061

support@newera.com

www.newera.com

Rev: 2019-6-24

1 Foreword

1.1 Copyright, Trademark and Legal Notices

1.1.1 Copyrights

1.1.2 License Agreement

1.1.3 Trademarks and Copyrights of Others

The following products and/or registered trademarks of International Business Machines Corporation (IBM) are referenced in this document: MVS, VM, RACF, z/OS, SYSPLEX, JES, VTAM, TSO, ISPF, ICKDSF, DFSMSdss, and DF/DSS. Other company, product or service names may be trademarks or service marks of IBM or other organizations.

1.2 General Information

1.2.1 Who Should Read this Document

Those given the responsibility to install, maintain, and use The Control Editor should read this document. It, in conjunction with The Control Editor User Guide, will explain in detail how The Control Editor is installed, configured, maintained and used. Specifically, this Getting Started Guide will provide product use exercises.

1.2.2 Other Documents and Resources

In addition to this document, new users will benefit from the content of these three additional documents:

- The Control Editor Read Me;
- The Control Editor User Guide;
- The Image FOCUS User Guide.

All of these documents are available in PDF format as downloads on the NewEra web site or can be requested directly by contacting NewEra Technical Support by email at the following email address: support@newera.com.

1.2.3 Online Help – PFK1

In addition to the information contained in this document and others, The Control Editor user may access an Online Help Tutorial for any given panel by pressing PFK1 once the panel is fully displayed.

1.2.4 Reporting Problems

When reporting a Control Editor problem to NewEra Technical Support, please provide the following information so that we may resolve the issue expeditiously.

- The JOBLOG/JCL/MESSAGE output from IFOM and IFOS;
- The contents of the NSECTLxx, NSEJRNxx and NSEENSxx members;
- An ISPF 3.4 listing of the Journal Datasets showing the allocation and DCB information;
- An ISPF 3.4 listing of the datasets in NSECTLxx.

1.2.5 Technical Support Information

Around-the-clock-support	NewEra Software is dedicated to providing the highest level of technical support to meet our customers' growing needs. In order to meet these needs, NewEra provides technical support, 7 days a week, 24 hours a day.
Reach us by Telephone during Business Hours	Please use the following phone numbers to reach our technical support staff during normal business hours (6 AM to 4 PM Pacific Time): • In North America, dial 1-800-421-5035 • Outside North America, dial 1-408-520-7100 • Support inquiries may also be texted to 669-888-5061
Reach us by Telephone during non-Business Hours	In case of an emergency, during non-business hours, phone the above numbers to receive instructions on how to contact a Technical Support Representative or a Technical Support Manager.
Sending Email	Our technical support staff can be reached by email at support@newera.com. Email messages will be answered by the next business day. Product technical questions or product recommendations may be sent via email.
Help through the NewEra website	You can access technical support from www.newera.com. Click the Support tab at the top of the screen to reach our Technical Support Request page.
Service Levels	NewEra is committed to providing the highest level of quality to our customers by adopting the following criteria for responding to customer requests: • All critical questions received by phone during working hours will be answered within 15 minutes of receiving the request; • Technical questions sent by email, or messages sent through our Technical Support Request page, will be answered by the next business day.
We Want Your Suggestions!	NewEra understands the significance of providing our customers with the highest quality support and welcomes all suggestions as to how we may improve Technical Support.

1.3 About The Control Editor

The Control Editor (TCE) is an optional licensed application of the Integrity Controls Environment (ICE). The leader of its development team and primary architect is:

Mr. Gordon Daniel, Director Software Development, NewEra Software, Inc.

Its intended purpose is to extend Integrity Controls Environment (ICE) and, in doing so, provide to users an ISPF editing platform from which they can both control and manage the access to and productively identify changes in critical system datasets and system configuration settings.

In this, the seventh release of The Control Editor (TCE), new Control Journal dataset formatting options are provided. Users may now optionally specify HFS/zFS increasing a single Journal's event storage capacity over one hundred-fold. A new External Notification Subsystem has been added that allows users to specify event notification rules that will keep critical staff notified of configuration changes as they occur in real-time.

As with prior releases the Administrative Functions of the Control Editor run only within ICE, while TSO user accessible Edit Events like: Edit, Rename, Delete, Restore and Submit can run in both the ICE and ISPF Environments.

1.4 System Requirements

1.4.1 Prerequisites

To use The Control Editor, you will need Integrity Controls Environment (ICE) 15.0 and above and z/OS V1R8 or higher. You will find the latest release of ICE at www.newera.com.

1.4.2 The License Key

A License Key is required to activate The Control Editor. Once the License Key is inserted, The Control Editor functions will be unlocked the next time you logon to the ICE Environment.

1.4.3 Releases Prior to Release 15.0 of ICE

If you are a current ICE user and have not yet upgraded to Release 15.0, special care should be taken when you do upgrade to 15.0 to remove all pre-existing ICE Libraries. All pre-existing Inspection Reports (logs) and Package/Blueprints (packages) are fully supported in Release 15.0.

1.4.4 Event Notification Service

To use IFOM with external notification, the minimum z/OS release level is z/OS 1.9.
At z/OS 1.9, the NSIMTC3 REXX exec must be installed in the system REXX SYS1.SAXREXEC dataset. For z/OS 1.10 or newer, the NSIMTC3 REXX exec can be installed in either the SYS1.SAXREXEC dataset or in a user defined system REXX dataset as defined with the AXRxx parmlib member.

The NSIMTC3 REXX exec is invoked through system REXX which uses a secondary address space to perform its work. The address space names used rotate through jobs named AXR01 - AXR08 and run under USERIDs of the same name. USERIDs AXR01 - AXR08 should be set up within the corresponding security product and should be set up with an OMVS security segment as well as an OMVS UID.

1.5 Things to look out for

1.5.1 Critical Relationship

There should be a “One-to-One” relationship between a Dataset Category/Class and the Valid Datasets assigned/associated with the Category/Class. This is considered a “Critical Relationship” to the integrity of the information captured in the Control Journals and displayed in the various Control Editor panels and reports.

1.5.2 User Access to Datasets

The Control Editor does not do any additional security checking when a user attempts to access a member, as any required security should already be in place. If the user does not have READ authority when the edit starts, then the user will get an open error. At exit (save), if the user does not have UPDATE authority to the member, then the user will get an open for output error. This is consistent with the way the normal processing of the ISPF editor works.

1.5.3 History Function Password and HelpText

When you first access The Control Editor History Functions, you will be asked to provide a password. The default password is AMAZING. In addition, you will want to be certain to update the History Function “HelpText”. To do this place the cursor under “HelpText”, shown in the upper right of the History Function Primary Menu and press enter. If needed use PFK1 for additional help.

1.5.4 External Security Manager Issues

The NSEJRNxx and NSECTLxx UPDATE (but is not needed for BROWSE or EDIT) function accessed via the Administrator Interface requires that the following (the example is for RACF) or equivalent changes must be made to the External Security Manager (ESM) settings where “userid” is the TSO user ID for each user that will give TCE Dynamic Update Authority.

```
RDEFINE FACILITY NEZ.NSEPARM.** UACC(NONE)
PERMIT NEZ.NSEPARM.** CLASS(FACILITY) ID(userid) ACCESS(READ)
SETROPTS REFRESH RACLIST(FACILITY)
```

1.5.5 ReadMe File

For additional assistance concerning product installation, review the “ReadMe” file associated with the product download.

1.6 Control Editor Limitations

This release of The Control Editor has the following restrictions and/or limitations. If you are uncertain as to how this may affect the operation and/or function of The Control Editor in your z/OS environment, contact NewEra Technical Support at support@newera.com for assistance.

- First, if you have extremely large datasets, there is a potential to exhaust memory during The Control Editor processing. You can change your memory allocation by modifying your IFOS region size (you will need to LOGOFF, then LOGON to ICE).
- Second, The Control Editor backs-up and monitors individual members from datasets that are FB(80) and PDS/PDSE which are text-based members. It does not process libraries with binary-based members (e.g. load modules) or sequential datasets.
- Third, there is split-screen support for The Control Editor under TSO. But, you must follow the instructions found in the Installation Section carefully to avoid problems.
- Fourth, when allocating the Control Journals using the configuration member NSEJRN00, follow your site standards for HLQs and SMS definitions (e.g. STORCLAS).

1.7 Recent Enhancements to The Control Editor

- The native RACF Command Set that can be monitored has been expanded to include all native RACF commands. Up to this release only the SETROPTS command set was supported. Native RACF Commands added in this release include:

ADDSD	CONNECT	RDEFINE	DELUSER	ALTDSD
ADDGROUP	PERMIT	DELDSD	RDELETE	ALTGROUP
ADDUSER	RALTER	DELGROUP	REMOVE	ALTUSER

- The MVS Operator Command Set that can be monitored has been expanded to include all SETxxxx Commands. Up to this release only the SETPROG, SETSMF AND SETXCF commands were supported. Operator Commands added in this release include:

SETAPPC	SETETR	SETIOS	SETLOGRC	SETSMS
SETCEE	SETGRS	SETLOAD	SETOMVS	SETSSI
SETCON	SETHS	SETLOGR	SETRRS	SETUNI
SETDMN				

- Edit Event Email Notification associated with member updates now includes a record-by-record listing of changes that impacted the affected member.

- Edit Event Email Notification event journaling has been enhanced to more completely record the identity of the member impacted by the originating edit event.

- Changes detected by The Supplemental Detectors are now grouped, for presentation purposes, in both Journal and History displays and reports, with all other detected changes using the Event Class Names defined below:

    - DTIOD – Detected Changes in the Configuration of Named IODF Datasets.
    - DTCHK – Detected Changes in Health Checker State/Status on Named Systems.
    - DTIOD – Detected Changes in Modules in Named Load Libraries.

- The Edit Descriptor may now be programmed, by dataset category, to be ACTIVE and therefore appearing only during a defined time interval during a 24-hour period.

- The Keyword Aliases NBLANK and EORDR have been added to shorten and represent, as needed, the Keywords NONBLANK and EDITORDR used in defining the Edit Descriptor.

- Controlled Member Restore functions have been added to the Primary Menu allowing access to the Controlled Member Restore Selection Worksheet.

- History Report functions have been enhanced to support both foreground and batch reporting of changes impacting all or selected Controlled Datasets.

- Event management has been enhanced to allow for the recording and display, in reports and notifications, of the member changes detected during an Edit Session.

- Edit sessions of Controlled Datasets have been updated to include enhanced support for the COPY, CREATE, MOVE and REPLACE primary commands including the display of appropriate Event Descriptors for each.

- Support for recursive use of the following native EDIT Command Line Syntax:

    - `EDIT`, `EDIT` *`member_name`* and `EDIT` (*`member_name`*)

    - When used from within either a TSO/ISPF or TCE Edit Session, the EDIT Descriptor is displayed and each recursive EDIT Event is independently captured and recorded.

- Update of the Control Journal Interface allows for the classification of Backups and Control Events across time. The prior Legacy Journal Interface is still supported.

- The Control Journal Interface has been enhanced to support Member Event Restore Operations. Each member in the Restore List can be confirmed for restore individually or the entire Restore List can be restored at one time.

- Journal Dataset Formats – A new configuration option supports the creation of ZFS/HFS formatted Control Journal Datasets. This new Journal Type extends the storage capacity of each Journal from maximum of 116 to 16,382 Backup or Change Events.

- Event Notification – A new configuration option supports the real-time notification of events via Email. Event, Recipient and Notification Content are configured using the newly introduced NSEENSxx Configuration Member.

- Enhanced Recording – Event Journaling automatically subdivides event recording into three segments: Event Identity, Body and Report. Each is progressively selectable when used in conjunction with Event Notification.

- Dynamic Reconfiguration - The NSECTLxx, NSEJRNxx and NSEENSxx configuration members may now be dynamically reconfigured via the Administrator's Interface. Configuration changes become effective immediately and do not require a restart of IFOM.

- Detected Changes - The identification of changes made outside the Integrity Controls Environment, Detected Changes, has been fully automated and now runs optionally at predetermined intervals. The process may be run at any time via the Administrator's Interface and automatically prior to Report or OSAudit Library updates.

- IFO Results Posting – The results of Production Image FOCUS Sysplex configuration Inspection and change detection, the Sysplex Audit Log, is now posted directly to the Control Journals at the end of each Production cycle. Optionally, the results of Supplemental Inspections (ISNMBRS, ISNLOAD, ISNCSDS) may also be posted.
- Report Libraries - A library of standardized z/OS configuration change reports (The Report Library) and z/OS Audit Reports (The OSAudit Library) is now available.
- Batch Reporting - All library reports may be updated in batch and selected reports sent via email to selected recipients.
- SUBMIT Capture – The submission of JCL during an edit session is now captured and Journaled.
- Operator Command Capture - Dynamic system changes implemented via the MVS Operator Commands - SET, VARY, SWITCH, START, STOP, CANCEL, QUIESCE, TRACE, SWAP, SLIP, DUMP, FORCE and MODIFY can now be optionally captured and limited to one or more originating sources – Started Task, Console, JOB or TSOUser and Journaled.
- SETROPTS Capture - Dynamic changes to RACF implemented via the SETROPTS Command can now be optionally captured and Journaled. Functions for ACF2 and Top Secret are implemented via Command Capture - MODIFY ACF2 and MODIFY TSS.
- ACTIVATE Capture – Dynamic IODF changes implemented via the ACTIVATE Command can now be optionally captured and Journaled.
- Ad hoc Event Logging – A system Event Trace Logging option has been added to assist in forensic system analysis.
- Transparent SCAN – JCL can be automatically scanned (TYPRUN=SCAN) for problems that could prevent successful JOB completion during an ISPF EDIT session.
- Stealth Mode – Optional configuration setting that will suppress the display of the Descriptor Window associated with ICE or ISPF events. Journal recording is unchanged.

1.8 Planned Enhancements

- Sysplex Journaling – A new configuration option is planned that will allow all Control Events occurring throughout the Sysplex to be consolidated and written to a single set of Control Journals.
- Functional Control – Control over access to the various ICE primary and secondary functions will be implemented using the External Security Manager (ESM) XFACILITY resource class.
- Support for Sequential Datasets, Journal Records greater than 80 bytes, OEDIT and the IBM Health Checker for z/OS.
- Additional Supplemental Detectors for detecting changes in DB2, RACF and CICS.

1.9 Solving Real-World Control Problems

- "…when we installed and customized the Control Editor we noticed that certain critical z/OS Control Points (Load Modules, IODF Dataset and the Status of the IBM Health Checker for z/OS) were not monitored. We discussed this with NewEra and were really pleased when they announced the availability of the Supplemental Detectors to fill these control gaps. Using the Detectors, we can now monitor each at intervals that we define: Health Checker hourly, Load Modules daily, IODF weekly. The details associated with specific detected changes are sent via email to the responsible team for follow-up. By automatically postings each detected change to the Control Journals we are assures a complete and accurate history is always at our fingertips. Thanks, NewEra.

- "…we recently outsourced the operational aspects of our z/OS environment and related LPARs. Of course, we still have oversight responsibility for the integrity of the entire IT environment including all the pieces we outsourced. While we have a really good service contract with them and they have all the necessary SAS70 Service Audit Documentation in place, we still had concerns about knowing what was actually going on with our business application platforms. We are absolutely concerned with z/OS configuration changes especially Parmlib Member Updates, Dynamic MVS Operator and RACF Policy changes. We put all these concerns to bed with The Control Environment's External Notification Service. Now, when a change takes place, we get notification of the change automatically by email. With The Control Environment we know the "Who, What and Why" details of each and every change in real-time. Oversight responsibility satisfied, z/OS integrity retained.

- "…we originally passed on The Control Editor because it was not able to support really large datasets, datasets containing in excess of 10,000 members that we wanted to backup and actively track for changes. We changed our minds however when we learned about the new zFS/HFS file support option. Using it we can now capture over 16,000 members in a single Backup Journal and/or over 16,000 discrete change events in a single Control Journal. This has really simplified the backup process in our shop and provided us with a reliable method of maintaining complete documentation of generational changes. In short, we have a complete audit trail of all member changes. Safe, secure, responsible that the way I feel about The Control Environment.

- "...my guys say that they don't make changes but then, I guess by magic, changes show up. I am happy to say that since we installed The Control Editor the number of unexpected and undocumented changes has dropped dramatically. With the continued help of The Control Editor someday we'll get it down to zero. No surprises."

- "…our system audit reviews are done as part of our financial audit process. We have been written up several times for not having adequate documentation of actual changes. We do a good job of documenting what we are *going to do* but not what we *actually did*. The Control Editor filled this hole in our change management process by requiring users to provide descriptive information, documenting each change at the point of the change using standard TSO/ISPF. No more negative audit findings."

- "…everyone knows that submitting JCL during a TSO/ISPF Edit session can open a big hole in z/OS system security. JCL can be edited and submitted, even by those without UPDATE authority, and then the Edit session cancelled. No one is the wiser and generally RACF, ACF2 and Top Secret are totally by-passed. This has been an open audit finding in our environment for some time. The Control Editor closed this hole for us. No more undocumented changes to or submission of our JCL."

- "…we have contractors coming in and out of here all the time. We give them pretty much the same access we give to our own system programming staff. Until we began using The Control Editor we had no idea what they were actually doing, what changes they were making. The TCE reporting and query functions resolved this completely. I now know who did what, to what and when."

- "…we give our operators lots of access to MVS system commands. This allows them to dynamically reconfigure our z/OS Sysplex as needed to meet demand. We have been hesitant to implement strict COMMAND class control for fear of locking them out of the system. Leveraging the non-invasive recording of SET and ACTIVATE commands provided by The Control Editor we now have a way to capture and analyze what our operators are doing. No lockouts, dynamic changes documented."

- "…I cannot tell you how many times I have had to get involved in a system security dispute between my Security Officer and System Programming Manager. Both are well intended; one wants more security of z/OS system changes; the other says no way. The Control Editor resolved this for me, for us. It was easy to set up and since it enhances ISPF it was a snap to learn. Security guy has lots of reports and the System guys are now on "Friendly Terms" with a compensating control. Everyone is happy."

- "...we've had a lot of turnover in the systems area in the last year or two so all of us have had to pitch in to keep things going. One area of real concern is the RACF policy settings. We lost our security guy and have not and may not be able to replace him. My team is stepping up and helping out, but we all know we need better control over the use of the SETROPTS commands. We were using The Control Editor for documenting z/OS Configuration changes and now with this new release we can easily extend its scope to include RACF as well. We all really like the added value."

- "…in our shop money is a problem and we are always on the lookout for ways to cut cost, it's a way of life. We were using what turned out to be a very costly Change Management system to control and document z/OS configuration changes. When we learned that The Control Editor could do a much better job at half the annual maintenance cost we were intrigued and started an evaluation. It turned out that The Control Editor does so much more than the system it's going to replace. More function, less cost, real value."

- "…we've been using Image FOCUS for years. Love it, cannot live without it. Last year we considered evaluating The Control Editor, but it was tough to build interest. Everyone seemed to be happy with our existing change management tool set. 6.0 changed all that. The automatic posting of the Sysplex Audit Log to the Control Journals now allows ICE to pinpoint both configuration problems and to detail the complete history of components changes. Better integration, better integrity."

- "…we're in the insurance industry, lots of regulation, lots of compliance issues: SAS70, SOX and NAIC. Our CFO studied them all and concluded that what we needed was one approach to change management that satisfied all requirements, generally stated as: what changed, who changed it and on what authority. After an extensive evaluation of available software tools, we selected The Control Editor for three specific reasons: lowest total cost of ownership, seamless integration into our change process and its full set of compliance reporting tools. Regulations satisfied, CEO happy."

- "...recently we were not able to restore a z/OS component and as a result encountered a major delay following a system upgrade. The post review meeting brought to mind three important rules of life: number one, remember to brush your teeth, number two, take your vitamins, and number three, ALWAYS make a backup of your z/OS configuration members *BEFORE* you make changes to them. Simple, straightforward, common sense advice. So easy to do, so easy to forget. Since we installed The Control Editor I don't worry about my guy forgetting about number three. The Control Editor ALWAYS creates a backup before it allows an update. Let mom take care of one and two, The Control Editor will take care of the backups."

2 Table of Contents

3 The Control Editor Evaluation Questionnaire

Company:_____	Tester:_____
Phone:_____	Email:_____
Today's Date:_____	Download Date:_____
Start Date:_____	Date Codes Expire:_____

3.1 Ten Steps to Installing Image FOCUS

□ Download Image FOCUS from the NewEra website. Patch level: _____
□ Upload install job to mainframe.
□ Configure and run the install job. Check return codes.
□ Run the ALLOC and BUILD jobs. Check return codes.
□ Put The Control Editor License Control Statements into PARMLIB member NSEPRM00.
□ Move IFOM and IFOS into your system PROCLIB.
□ Update the Image FOCUS Procs. Image FOCUS HLQ: _____
□ Set up an Image FOCUS APPLID.
□ Start IFOM.
□ Log onto the Image FOCUS APPLID.

3.2 Ten Steps to Using The Control Editor

□ Log onto the Image FOCUS VTAM APPLID.
□ Select the Control Administration/Selection Option.
□ Select and use the Dataset Option to display the Control List.
□ Select a Dataset from the Control List displayed.
□ Select and Update a Member in a Controlled Dataset.
□ Access and Update a Member in a Controlled Dataset using TSO/ISPF.
□ Select and use the Journal Option to view Update Events.
□ Select and use the Actions Option to view and Update Configuration Members.
□ Select and use the Actions Option to detect and capture unaccounted for changes.
□ Select and use the History Option to display reports and query Control Journals.

Problems? Contact NewEra Software technical support (support@newera.com)

4 Image FOCUS Installation

The installation of Image FOCUS is defined in the Image FOCUS User Guide, which is a separate document included with the product. As you proceed with the install, the following can serve as a checklist and provide tips and suggestions. After the installation process has been completed, we will address the set up and execution of Image FOCUS later in this chapter.

4.1 Image FOCUS Terms and Definitions

The following are some basic definitions of terms used in this document and in **Image FOCUS** panels and screens.

- **Blueprints:** Blueprints are copies of the components extracted during an inspection by the IFOBG process. They are stored when a change has been detected to any component in the IPL process. These Blueprints are used to identify and track changes to the members, and datasets that define a Sysplex, Image, subsystem or user-defined data source.

- **IFOBG:** IFOBG involves the running of the inspection process under the control of a provided started task using interval timing to run unattended inspections in BACKGROUND (see "Production Selection" below).

- **IFOM:** The IFOM procedure creates a MASTER address space that will control all **Image FOCUS** users. This address should be started after an IPL and must be available in order for users to access the **Image FOCUS** VTAM Application.

- **IFOS:** The IFOS procedure is used when a user logs onto the VTAM Application. A separate address space is created for each user.

- **Inspection:** An Inspection involves the processing of the IPL path and applicable rules for the IPL and startup of a Sysplex, Image or Subsystem. It includes key components such as PARMLIB members, PROCLIB, and JES, VTAM, TCP/IP and CICS definitions.

- **Packages:** Packages are a dataset, one for each inspection request, that contain the generations of Blueprints.

- **Production Selection:** The Production Selection involves the set up and control of the IFOBG started task and is used for review and use of the Blueprints. It is used to monitor the integrity of a Sysplex or Image, detect changes and provide notification of status based upon the results of an inspection.

- **Recovery Selection:** The Recovery Selection provides access to ISPF through the **Image FOCUS** product.

- **Workbench Selection:** The Workbench Selection involves the setup, management and execution of inspection requests. This Selection includes analysis capabilities and interfaces into more advanced functions and services.

4.2 Installation Checklist – Getting Ready

The installation process begins by requesting the Image FOCUS Install Job (a sequential dataset) from the NewEra Software website.

- **Download request:** From the www.newera.com homepage, select "Evaluators - Download Image FOCUS", and follow the instructions.

- **Open the email:** You will receive an email from NewEra Software that contains a weblink to download the Install Job (sequential dataset).

4.2.1 Typical Evaluation Email from NewEra

From: ahr@newera.com [mailto:ahr@newera.com]
Sent: Monday, September 18, 2017 3:50 PM
To: new@evaluator.com
Cc: support@newera.com
Subject: IFO Evaluation

Dear:Evaluator, Your Company
Date:09/18/17 - 15:57:51

Subject:IFO Evaluation

Thank you for your interest in NewEra and our Products. We are very pleased that you have decided to begin an evaluation. If at any time should you need assistance, please contact us.

Follow the link below to reach your Image Focus Evaluation Resources.
(see your download email for the actual link)

Regards,

Technical Support, NewEra Software
mailto:support@newera.com

- **Click on the web link within the email:** A special NewEra Software webpage will appear with authorized downloadable Authorized Application Name(s).

Authorized Application Name	Download	Read Me	User's Guide
---------- --	----------	----------	----------
Image FOCUS Core Rel_150_Lev_Pxx	Click	Click	Click

- **Locate the links listed on the webpage:** Towards the bottom of the webpage, locate the Authorized Application Name(s). There are links for Download (Install Job dataset), ReadMe, and User Guide for each authorized application.

  In this example the application is "Image FOCUS Core Rel_150 Lev_Pxx" (where "Pxx" represents the patch level). The Application Names will change with new releases and new patch levels.

- **Download and save the datasets:** Click on the Download, Read Me, and User Guide links for each authorized application. Save these datasets onto a hard drive (local or network). Note that the Image FOCUS "Download" file is the Install Job, and has an ".nez" file extension.

- **Allocate the Install Job dataset:** Allocate a dataset for the Install Job on the mainframe. The Install Job space requirements are listed below:

  SPACE=(CYL,(35,5)),LRECL=80,BLKSIZE=6160, RECFM=FB

- Copy the Install Job to the mainframe: Copy the Image FOCUS Install Job dataset to the mainframe. Note that the file must be transferred in Binary. Verify that the last line contains only two @ signs.

- **Edit the Install Job on the mainframe:** Change the Jobcard parameters to conform to your site-specific standards. Do not renumber this member, and do not make global changes. Modifications should not be made past line 27 of this member.

- **Specify and Record HLQ and Volume Names:** Specify the HLQ and Volume names for the Image FOCUS datasets within the Install Job. Record them here for future reference:

  &nssprfx =_____

  &dskvolu =_____

- **Submit the Install Job:** Exit the Edit Session before submitting the job. The Install Job creates a library called HLQ.INSTLIB (where HLQ is replaced by the &nssprfx symbolic). Verify the job return codes.

Do Not Submit this job from ISPF Edit. If you experience a B37 space abend when you submit the job, this likely is due to submitting the job from ISPF Edit. Save and Exit the ISPF Edit session and submit the job from the TSO command line (ISPF Option 6 - Command Shell), or from ISPF Option 3.4.

- **Edit and submit the member ALLOC:** This job allocates the Image FOCUS datasets. Change the Jobcard parameters to conform to your site-specific standards (no other changes required). Verify that the HLQ and Volume names are correct and submit the job. Verify the job return codes.

- **Edit and submit the member BUILD:** This job builds the Image FOCUS product (populates the Image FOCUS datasets). Change the Jobcard parameters to conform to your site-specific standards (no other changes required). Verify that the HLQ and Volume names are correct and submit the job. Verify the job return codes. If you receive a B37 abend, an ISV intervention is managing the blocks (increase the sizes and restart).

```
DSLIST - Data Sets Matching IFO.IFOX

COMMAND ===> _____________________________________ Scroll ===> PAGE
Command - Enter "/" to select action ..............Message ....... Volume
------------------------------------------------------------------------------
__ IFO.IFOX.INSTLIB
__ IFO.IFOX.IPLCHECK.SYSTEM.LOG
__ IFO.IFOX.IPLALT.SYSTEM.LOG
__ IFO.IFOX.LOAD
__ IFO.IFOX.PACKAGE.INDEX
__ IFO.IFOX.PARMLIB
__ IFO.IFOX.PROFILE
__ IFO.IFOX.REPORT.INDEX
__ IFO.IFOX.SISPCLIB
__ IFO.IFOX.SISPMENU
__ IFO.IFOX.SISPPENU
__ IFO.IFOX.SISPTABB
__ IFO.IFOX.SISPTABL
__ IFO.IFOX.USERLIB
********************* End of Data Set list ******************************
```

- **Authorize Load Library:** Follow the install instructions found in the Image FOCUS User Guide to authorize the LOAD library. Dynamically add this library to the APF list or add the dataset to the correct PARMLIB member. Then do a refresh of the APF list or do an IPL.

  Standard Command to dynamically add an authorized library (issue from an operator console or an equivalent utility):

  ```
  SETPROG APF,ADD,DSNAME=nnnn,VOLUME=volser
  ```

Standard Command to refresh the APF list: (issue from an operator console or an equivalent utility):

```
SET PROG=xx
```

- **Specify Image FOCUS Licensing Information:** Follow the Image FOCUS User Guide instructions for either "Fully Pre-Authorized" (no control cards needed) or "Self Authorized" (evaluation keys are required in PARMLIB member NSEPRM00).

- **Review additional Installation Checklists:** Review the additional installation checklists found in this chapter and follow the instructions if they apply to your environment.

4.3 Installation Checklist - Multi-Users using a VTAM Application

If you plan to allow multiple Image FOCUS users, you will need to create a VTAM application for Image FOCUS. Remember that you will need to vary the APPLID active before it can be used. If you choose not to create and use a VTAM application, Image FOCUS can only be used in what is referred to as Recovery mode, which is a single user in dedicated terminal mode only.

4.3.1 Setting up VTAM APPLID

When installing Image FOCUS as a VTAM application to support multiple users, you will need to edit the following procedures and copy them into one of the PROCLIB datasets. For more information, see Section 8 of the Image FOCUS User Guide.

- **IFOM - Proc IFOM:** a started task that will remain active until stopped. The IFOM procedure is used to create a MASTER address space that will control all Image FOCUS users. This address should be started after an IPL and must be available in order for users to access the Image FOCUS VTAM Application. The IFOS procedure is used when a user logs onto the VTAM Application. A separate address space is created for each user.

- **IFOS - Proc IFOS:** a started task that is started by IFOM when each user logs on. This task will self-terminate when the user logs off.

4.3.2 VTAM Setup Tips

- You may need to add this application to your VTAM session management product.
- Verify that VARY ACTIVE was specified for the APPLID.
- If the APPLID is changed, validate the changes throughout.
- IFOM must have VTAM APPLID (IFO) specified in PARM (PARM line must have a comma in column 71).

- You may need to define SUBS (subsystem) IFO1 to the resident security system (RACF, etc.). This subsystem is needed for IFOM.
- Users must have read/write access. Otherwise “Not Authorized to create dataset” error messages may be issued during START IFOM.

4.4 User Logon and Security Considerations

It is important to remember that as a user logs on to Image FOCUS, in either VTAM or recovery mode, the user should use their normal USERID and PASSWORD. Image FOCUS will make the necessary SAF calls and verify security access with the resident security system. Access to Image FOCUS can be restricted in this way.

The user can enable an exception to this as described in Section 8 of the Image FOCUS User Guide. Also, consider security rights for the Image FOCUS address spaces. They will need access to all of the datasets that will be examined during an IPL inspection. This will include PARMLIB(s), PROCLIB(s), JES, VTAM, TCP/IP, and CICS datasets.

4.5 The Next Installation Step

The next step in the installation will be to update the PARMLIB dataset for Image FOCUS. The member &nssprfx.PARMLIB(NSEPRM00) controls the execution of IFOM and IFOBG and contains control statements for the temporary and permanent licensing of Image FOCUS provided to you by NewEra Software.

If you have not received these control statements, please email support@newera.com or call 800-421-5035 or 408-201-7000.

4.6 The State of the Install

Completing the installation to this point will allow the IFOM address to execute, users to logon to the VTAM application, and for you to continue with the additional steps need to complete the installation of The Control Editor as described below.

4.7 Control Editor Specific Installation Steps

Now that the Image FOCUS base has been installed you are now ready to complete the installation of The Control Editor.

4.7.1 Setting up TCE for TSO/ISPF Users

The Control Editor Users Interface Functions are optionally available under native ISPF. They are activated as follows:

First, verify that you have the CE#ALLOC and CE#BUILD in your HQL..INSTLIB dataset.

Submit CE#ALLOC from the HLQ..INSTLIB dataset. Verify that the return code is Zero (0).
Submit CE#BUILD from the HLQ..INSTLIB dataset. Verify that the return code is Zero (0).

Second, after the jobs are run, verify that the following datasets exist (necessary for CE/TSO):

- HLQ..CETSO.LOAD - load modules in non-APF authorized library
- HLQ..CETSO.LPALIB - load module to be loaded into LPA and/or LPALST
- HLQ..SISPCLIB - REXX programs
- HLQ..SISPMENU - ISPF messages
- HLQ..SISPPENU - ISPF panels

Third, make these two dynamic system changes.

- Update IKJTSOxx to add NEZCHKT as an authorized TSO command.

- Invoke these operator console commands:

```
set ikjtso=xx
setprog lpa,add,modname=nezchkt,dsname=HLQ..cetso.lpalib
```

Fourth, run these three REXX programs from the ISPF Command Shell (SPF Option 6).

Found in the HLQ..SISPCLB2 library these programs MUST be edited during the install so that the dataset names inside the programs match the ones used in the install of ICE.

4.7.1.1 CETSO

This command runs the same Control Editor function as ICE, but it begins at the Dataset Panel.

4.7.1.2 CEINIT

This command sets up the Control Editor environment including the ISPF EDIT macro so that any dataset edited with TSO will invoke the Control Editor if the dataset is in the control list.

4.7.1.3 CETERM

Removes the Control Editor environment and ISPF EDIT macro setup.

Finally, to launch these programs from ISPF Option 6, use the following command format:

```
EX 'HLQ..SISPCLB2(CExxxx)'
```

4.7.2 Transparent ISPF

There are many ways to integrate The Control Editor functions into ISPF transparently to the end user. In this section one method is introduced. We welcome your comments and feedback on this and other methods of integration.

The ICE INSTLIB members SAMC01A and SAMC01B contain the instructions and sample job to allocate a dataset and run the ISPF Configuration Utility. It is a best practice to be certain that The Control Editor is functioning correctly within the ICE Environment before you attempt transparent integration into ISPF.

Once The Control Editor installation has been validated, do the following:

Follow the instructions found in INSTLIB member SAMC01A as summarized below:

- Allocate Datasets to install the ISPF Configuration File. Submit JOB SAMC01B from the INSTLIB dataset and verify a zero completion code.
- Set up a System-wide Edit Macro for the Control Editor. Type “TSO ISPCCONF” on a TSO Command Line and press <ENTER>. Use the ISPF Configuration Utility panel to create/modify settings and build the configuration module.
- Update TSO Logon PROC. Add the CE-TSO datasets to the library concatenations as detailed in INSTLIB member SAMC01A.
- Verify the installation. First log-off, then return to TSO. Edit a Controlled Dataset and verify that the Control Editor is being used.

4.7.3 External Notification Services

To use IFOM with external notification, the minimum z/OS release level is z/OS 1.9.
At z/OS 1.9, the NSIMTC3 REXX exec must be installed in the system REXX SYS1.SAXREXEC dataset. For z/OS 1.10 or newer, the NSIMTC3 REXX exec can be installed in either the SYS1.SAXREXEC dataset or in a user defined system REXX dataset as defined with the AXRxx parmlib member.

The NSIMTC3 REXX exec is invoked through system REXX which uses a secondary address space to perform its work. The address space names used rotate through jobs named AXR01 - AXR08 and run under USERIDs of the same name. USERIDs AXR01 - AXR08 should

be set up within the corresponding security product and should be set up with an OMVS security segment as well as an OMVS UID.

4.7.4 Installing the History Functions

In addition to the download link you received and used to install ICE, you should also have received an email download link with the subject of AMR/PLUSONE Evaluation Key. This second link gives you access to TCE History Function modules ISNEDIT and ISNTEXT.

To begin the download process, click on the download link that says:

ISNEDIT - Transaction History and Auditing

This click will start downloading of the following file:

ISNEDIT_IFO_Rel_GA_Lev_14._WEBRAW.NEZ

When the download is complete, rename the file by changing the extension from .NEZ to .EXE. Next, expand the file to extract its contents; generally, a double click of the file will do this automatically. The expansion will reveal the full Image SENTRY collection of 18 separate files. For the TCE History Functions you need both the ISNEDIT.BIN and ISNTEXT.BIN. Move both files into the IFOhlq.IFOllq.USERLIB dataset that was automatically created during the ICE installation.

When you first access the History Functions, you will be asked to provide a password. The default password is AMAZING. In addition, you will want to be certain to update the History Function “HelpText”. To do this place the cursor under “HelpText”, shown in the upper right of the History Function Primary Menu, and press enter. If needed, use PFK1 for additional help.

4.8 Other Image FOCUS Components

The installation of other Image FOCUS components can be done on an as needed basis, but we will not implement them in these initial Getting Started tests.

The INSTLIB dataset contains an index member, $INDEX, that explains the use of the other members in this dataset where these other members add further functions. They include running the Image FOCUS inspections in batch using IFOBAT, providing sample custom inspectors such as IFOREXX, and with MAILINST enabling an email service interface to Image FOCUS.

Before you begin to install additional components, please review the members carefully in order to make certain you make productive use of their capabilities.

4.9 Additional Customization

Additional customization can be done for either a single user or multiple users if required and the INSTLIB dataset contains sample profile programs for this purpose.

4.10 The Next Step

Now that the installation of the basic functions of Image FOCUS has been completed, we will address the use of The Control Editor.

5 The Control Editor Walk Through

This getting started guide is to be used to working guide for a new TCE administrator through:

- The functional setup and use of TCE,
- The testing of the setup and availability of TCE features,
- Acquaint the TCE administrator and new users with TCE functions.

5.1 Other TCE Documentation

The administrator for TCE should also have available the full TCE User Guide for version 15.0, sections 3 and 4 should be reviewed, and the User Guide for Image FOCUS (IFO) 15.0. Like Image FOCUS TCE is an application within The Integrity Controls Environment (ICE) and both IFO and TCE need to have been installed prior to using this guide. It is also important to have the installer review section 7.3.5 of the TCE User Guide to enable a function called The External Notification System (ENS). We will include steps to use ENS later in this guide.

5.2 Installation Options

During the installation of TCE a choice was provided as how to activate TCE. These are explained in section 6.2 of the TCE User Guide. In order to proceed we must know which install method was used, the temporary method, using CEINIT, or the install for native ISPF.

5.3 Logon Alternatives

If the install for native ISPF was selected, skip to 4.0.

If the use of the temporary activation was selected, logon onto a TSO/ISPF session and select option 6, Command. Enter the following command:

```
ex 'hlq..SISPCLB2(ceinit)'
```

Where the hlq is for the datasets where the ICE 15.0 and TCE 15.0 datasets were installed. This will activate TCE for this user only and only during this session. Logging off, or entering the following command, will terminate TCE.

```
ex 'hlq..SISPCLB2(ceterm)'
```

5.4 Getting Started Exercises

The ten primary and one bonus exercise that follow in this section will help you to gain a fundamental understanding of the capabilities of The Control Editor. Once you have worked through these exercises you will have the foundation need to exploit the many functions of TCE.

5.4.1 Capturing PARMLIB Change Events

By default, TCE will protect the PARMLIB concatenation datasets. This can be changed and is defined in the NSECTL00 member of the ICE parmlib dataset. To test the capture of PARMLIB member change events do the following:

- Using ISPF option 3.4 select one of the parmlib datasets for edit. Select a member and make a small change to that member.

- Now save the changed member. You should be presented with a default panel with an additional line like this:

```
---------------------------THE CONTROL EDITOR-----------------------
SYSPLX:SVSCPLEX SYSNM:S0W1     USRID:GBAGS1  TIME:12:07:08 DATE:09/24
----------------------ENTER DESCRIPTIVE TEXT BELOW--------------- Edit
PROJECT NUMBER

CHANGE REQUEST NUMBER

COMMENTS
```

- Now without supplying any additional information, try and save the member again and you will see a panel like this:

```
Edit Descriptor Template Line Data Entry Underrun

DESCRIPTOR DATA DETECTED ON 0 ENTRY LINE(S)

TEMPLATE SYSTEM.PARMLIB   REQUIRES 1 UPDATED LINE(S)


If there are an insufficient number of blank lines in
the original descriptor line block to accommodate the
specified update line requirements, issue the CANCEL
command to terminate and exit this edit session.


Press END to exit
```

This panel is informing you that as a default for changes made to this PARMLIB dataset a policy has been defined in the NSEJRN00 member that some information must be

provided on the prior panel. Return to the prior panel with a PF3 and now add some text to one or more of the new lines, line 5, 7 or 9.

- After entering this information, again save the member.

The member will be saved by ISPF into the correct dataset, and a record of this 'Event' has been recorded into the journal datasets, maintained by TCE. The results of this will be viewed in exercise 2.

This process will be the same for all type of events, for all the datasets that have been defined to TCE.

5.4.1.1 Creating a Dataset Control List

The definition of datasets is made with the NSECTL00 member but by default we have the PARMLIB datasets being protected. If you wish to add more datasets, please review that member and the TCE User Guide section 7.2.

5.4.1.2 Defining the Descriptor Window

The definition for the Descriptor fields and controls are in the NSEJRN00 member and can be changed by reviewing that member and section 7.1 of the TCE User Guide.

The type of events that can be captured by TCE are defined in section 5.1 of the TCE User Guide. It is suggested that you add more datasets to those being protected by TCE, and to create policies for each category, as needed. This can be done by updating the parmlib members, or via the TCE administrator interface from the ICE panels; Exercise 5.4.3.

5.4.2 View the Recording of Change Events

Logon to the ICE VTAM application, and from the main panel select option 'C' Control Editor. Then select 'J' for journals. You will see a list of journals, some of them marked as 'BACKUP' journals. These contain the baseline copy of all members in the PARMLIB dataset concatenation. You will also see a journal marked as 'OPEN'. Select the OPEN journal. You should see one or more lines like this:

```
SYSTEM.PARMLIB     SE  COMMNDP1   USERID   09/25/2017 11:24:29  SUCCESS
```

By selecting this line, you will see the details of the changes made in exercise 5.4.1.

As you attempt other changes, or other events, they will be recorded into the 'OPEN' journal and they can be viewed in the same manner. The management of the journals is defined in the NSEJRN00 member as documented in section 7.1 of the TCE User Guide.

In addition to viewing the events in this way, TCE also provides a complete reporting system for both online and batch reporting; query and selection capability are also included with TCE and is fully documented in section 8.4, History Functions, of the TCE User Guide.

5.4.3 Changing TCE PARMLIB Member NSECTL00

Return to the TCE main panel and select option 'A' Actions. This will take you, to the panel where commands can be entered to close and open new journals, reconfigure TCE parmlib members, and on demand locate any undetected changes that may have been made to datasets under the control of TCE. This is one of several methods TCE provides to detect changes.

Choose option 'F' Config. You will now see a panel with the NSECTL00, NSEJRN00, and the NSEENS00 members. Each of these can be requested and changed from this panel, but at this time select 'C' for the NSECTL00 member. Following the example in the member, or the documentation in the TCE User Guide section 7.2, add a category with one or more datasets and save the member. This is done by requesting 'E' Edit of the 00 member.

After the updated 00 member has been saved, request 'U' update of the 00 member. TCE will then proceed to create a BACKUP journal(s) for the members in this (these) dataset(s) and will record events that affect these members.

At this time, you can repeat exercises 5.4.1 and 5.4.2 using the dataset(s) you have added to the NSECTL00 member.

5.4.4 Recording ESM Security Policy Events

Return to the NSEJRN00 member and near the bottom of the member you will see the following statements which control the activation of ESM capability of TCE.

```
*************************
* SECURITY OPTIONS      *
*************************
ESMINTERCEPT     OFF
*RACFCMDINTERCEPT ON|OFF
*TSSCMDINTERCEPT ON|OFF
*ACF2CMDINTERCEPT ON|OFF
```

Change the ESMINTERCEPT value to ON, and the same for the statement relevant to your security system. If you are using RACF, there is no need to make more changes to this member. If you are using TSS or ACF2, you will need to add a statement in the event capture options section of this member, such as MODCMD ACF2, or MODCMD TSS.

Now any changes to the ESM that result in a SETROPTS for RACF, or a Modify to TSS or ACF2 will be captured and recorded in journals, then reviewable as in the prior exercises.

The full explanation of these Security Option keywords is described in Section 7.1.9 of the TCE User Guide.

5.4.5 Recording MVS Command Events

Following the steps in exercise 5.4.3, select NSEJRN00 member for edit. Review the documentation for this member in section 7.1 of the TCE User Guide and comments within the member. Near the bottom of the member you will find the following statements:

```
**************************
* EVENT CAPTURE OPTIONS   *
**************************
OPERCMDINTERCEPT OFF
MODCMD   LLA
MODCMD   OMVS
SETCMD   SCH
SETCMD   IKJTSO
SETCMD   SETPROG
SETCMD   ACTIVATE
SETCMD   SETROPTS
MISCCMD  VARY EXCLUDE(JOB,STC)
```

Change the value for OPERCMDINTERCEPT from OFF to ON. This will activate command capture by TCE and will record any use of the commands listed into the 'OPEN' journal. Please remember that this is a short list of possible commands and sub commands that can be captured. Save the member and select 'U' update the NSEJRN00 member.

Try several of the commands from any MVS console service. Then as in exercise 2, you can review the journals for these events as well as report on them using the reporting and query facilities.

5.4.6 Activating the External Notification System

Again, using the instructions from Exercise 3 and 4, select the NSEJRN00 member for edit. Find these statements near the bottom of this member:

```
*************************
* EVENT NOTICE OPTIONS    *
*************************
EXTERNALNOTIFICATION OFF
```

Changing the OFF to ON for this statement which will enable this function within TCE. Save then update the NSEJRN00. The control definitions for this function are contained in the NSEENS00 member, which we will now need to edit and update as you have done in the prior exercises.

Documentation for this member can be found in section 7.3 of the TCE User Guide and in comments within the member.

At the top of the member several changes will need to be made to adhere to your installation and email support from the LPAR where we are executing. Also please remember to remove the * in column 1 of any statement needed so that it will be an active statement and not considered a comment. By removing the * from the first example set of ACTION statements, and repeating exercise 1, an email will be sent as you have directed, and entries will be made to record those email events into the journals, which can be viewed by repeating exercise 2.

```
METHOD EMAIL
TO       recipient@yourcompany.com
FROM     sender@yourcompany.com
SERVER   smpt.mail.server
TCPIPJBN TCPIP
SUBJECT  'Default subject'
PORT     25
TIMEOUT  45
DEBUG    OFF
DEBUGDSNHLQ hlq.llq.DEBUG
TEMPDSNHLQ  hlq.llq.TEMP
METHOD .END
*-------------------------------------------------------------------*
*   Define CATEGORY(SYSTEM.PARMLIB) ACTION                          *
*                                                                   *
*   OBJ(ALL) indicates all SYSTEM.PARMLIB EDIT, DMDEDIT, and SUBMIT *
*   events are captured for notification.                           *
*   SCOPE(REPORT) indicates that the full edit journal entry is     *
*   provided as an attachment to the transmitted e-mail.            *
*                                                                   *
*   Override the default EMAIL METHOD FROM.                         *
*                                                                   *
*   DEBUG ON captures and saves debug information to a saved dataset *
*   using DEBUGDSNHLQ prefixed dataset names, again using the       *
*   EMAIL METHOD default.                                           *
*-------------------------------------------------------------------*
ACTION CAT(SYSTEM.PARMLIB) METHOD(EMAIL) OBJ(ALL) SCOPE(REPORT)
FROM     sender@yourcompany.com
DEBUG    ON
SUBJECT  'SYSTEM.PARMLIB edit update'
ACTION .END
```

5.4.7 Detecting Changes Outside ISPF Edit Points

Until now all the exercises have dealt with capturing and recording events as they have occurred, the edit of a member or the use of a command. But there are times when changes are made through access other than ISPF. These can be changed by the use of a batch job or FTP, as examples. TCE has several methods of detecting changes that may have been made to the members in a controlled dataset.

- The first and easiest is a simple compare when a member is opened for edit. TCE compares the content of the member against the stored baseline/backup of the member. If TCE detects a change, a new backup is made, and a journal entry made. The entry type

for the new entry will be 'DF'. A list of all types and definitions can be found in section 8.2.7 of the TCE User Guide.

- The second method that TCE uses to detect changes is the automatic running of a background task with a timer that looks for changes to the META records for each member in a Controlled dataset. This is explained more in section 5.1.8 of the TCE User Guide. The task is named and controlled by the NSEPRM00 for ICE in the hlq.hlq.parmlib dataset for ICE.

- The third method TCE uses to detect change is by command request. On the panel discussed in exercise 3, where we selected an 'F' to do the configuration changes, you will also see an option 'D'. By entering this command, TCE will compare the META data for each controlled dataset and will detect and record any changes made to any of these datasets, creating new backup journal entries, Type 'DF'.

Any of these methods can be tested simply by doing one of the following:

- If you have started TCE with the CEINIT command, simply logoff or enter the CETERM command under OPTION 6. This will stop TCE. Then, log back onto your ISPF session or proceed by making an EDIT to a member in one of the PARMLIB datasets.

  Now reenter the CEINIT command and try one of the methods for detecting changes explained above. The easiest is to select the same changed member for edit. Whether or not you make further changes, you should be able to access the journal display and see the new type 'DF' record for the member as the last entry in the open journal.

- If you have not started TCE with the CEINIT command but have used the install for native ISPF users, you will need to make this change in some other way, understanding that TCE will capture and record all edit events against a controlled dataset by all ISPF users.

TCE will also automatically detect changes anytime a report or query is requested so that the results of the query and the content of all reports are current and accurate.

5.4.8 Setting up TCE Reporting Capabilities

Now that we have captured and recorded event details into the journals for TCE, we now must begin to think about how this information can be used and shared. This is be done by using the reporting and query functions available under the 'H' History selection found on the main TCE panel. The use and setup of the History function is documented in section 8.4 of the TCE User Guide.

Once again after logging onto the ICE VTAM application, select option 'C', TCE Administration and the option 'H' History. At this point you will be asked to provide a valid password. The default password is the word 'AMAZING'. In addition, while viewing this panel you will want to be certain to update the History Function "HelpText". To update the text place the cursor under "HelpText", shown in the upper right of the panel, and press enter. If needed, use PFK1 for additional help.

Proceed to the panel to select option 'R' Reports. This will take you to the Journal report library setup panel.

To create the first set of reports, place today's date in the field:

```
.. Date Range Upper yyyy/mm/dd
```

The lower date range field need not be specified. Leaving it blank will result in ALL journal records to be included in the reports. In the future, you may wish to use a lower date range to reduce the reporting window to a selected time frame.

Now at the bottom right of this panel you will see the field:

```
.. Update Library
```

You can either place an 'S' and select this field or use the advanced feature of simply placing your cursor on this field and hitting enter.

This will create a library of reports of various titles and level of detail and when complete will present a continuation message on the screen, asking for acknowledgment by using the PF3 key.

Now you are free to review the reports by using again the 'S' select line command or the advanced cursor placement feature.

You can at this time also review and setup the reporting to be done with a batch process by selecting the field marked '`.. Batch Monitor`' and following the setup as described in the TCE User Guide section 8.6.

5.4.9 Using the Query Capabilities of TCE

Returning to exercise 5.4.8 and the panel where you had previously selected the 'R' Reports option, now select the 'Q' Queries option. Documentation for the Query function can be found in section 8.4.5 of the TCE User Guide.

The panel displayed after selecting 'Q' Query displays field name for data elements in the journal records. This panel has Boolean logic to process the query selection request and multiple fields/criteria search.

For example, on the top line under the 'Member' you can specify the member that you have been changing during these exercises. If you are unsure of what values for any field would be valid you can select a list of the available values by placing your cursor on the field name and hitting enter.

So, by placing your cursor on the word 'Member' and hitting enter, you will see a list of the member names recorded into any of the journals created by TCE.

After supplying a member name, hit enter and a worksheet display will be created that will allow you to sort the display by any column or further reduce the data displayed by typing a value at the head of any column or selecting a value within a column.

Feel free to experiment with this display and use the commands available in the 'OPTION' field to generate reports or export data from the displayed information.

- REPORT PRINT,COPY,MAIL Print, Copy or Mail Full formatted report.
- EXPORT PRINT,COPY,MAIL Print, Copy or Mail Comma delimited data.

You should also return to the 'Journal/Member History Search' panel and try the Boolean logic capability by also specifying your userid along with a member name and/or any other combination you wish to try.

5.4.10 Using the Member RESTORE Function

We have seen how TCE can capture and record events. The reporting and query functions can allow us to share and document those events. Now let us review how we can use the records in the journals as a measure of protection from problems with the automatic backup of members when they are changed or deleted. This is a simple exercise that will walk you through the steps to perform a RESTORE of a member to a prior version that was captured and saved automatically by TCE.

Once again logon to the ICE VTAM application, select option 'C' Control TCE Administration. In prior exercises we have used the 'J' Journal path to view the recorded events that will also allow for restore. But we will now use a different path to RESTORE a prior version of a member.

Select option 'D' from the Administration Selection panel. This will display a list of categories that you have defined in prior exercises or that were automatically created by TCE. Select the

SYSTEM.PARMLIB category with an 'S'. You will now see a panel that lists ALL the datasets in this category and you can select a single dataset with an 'E', or simply hit enter without making a selection and a full list of the members stored in the journals will be displayed.
The description of the panel and its use can be found in section 8.1.3 of the TCE User Guide.
Scroll down the list of members until you see the member that has been changed in prior exercises. It should have a value of UPD displayed showing it has been changed since the first backup was taken.

Now enter the line command 'HS' History Summary. The display will be of ALL the recorded events for this member. Entering the line command 'C' by 2 entries will compare them, an 'S' will display the member, but the 'R' will allow you to restore that version of the member into the original dataset.

Place the 'R' before the original member and hit enter, a confirmation panel will appear, and after confirmation you should once again see the panel created for TCE where documentation for this event may be required. This was setup in exercise 1.
After providing the required or optional information, the member will be restored, and a new event record added to the open journal. This can now be reviewed and reports showing this activity can be updated and created.

5.4.11 Bonus Exercise – Scanning JCL

To be done when working with a JCL member in a controlled dataset.

On the command line, type SCAN, and enjoy the short cut.

5.5 Congratulations

This concludes your testing of the fundamental capabilities of The Control Editor. With the examples and work you have done up to this point, you will have a good foundation for your continued use.

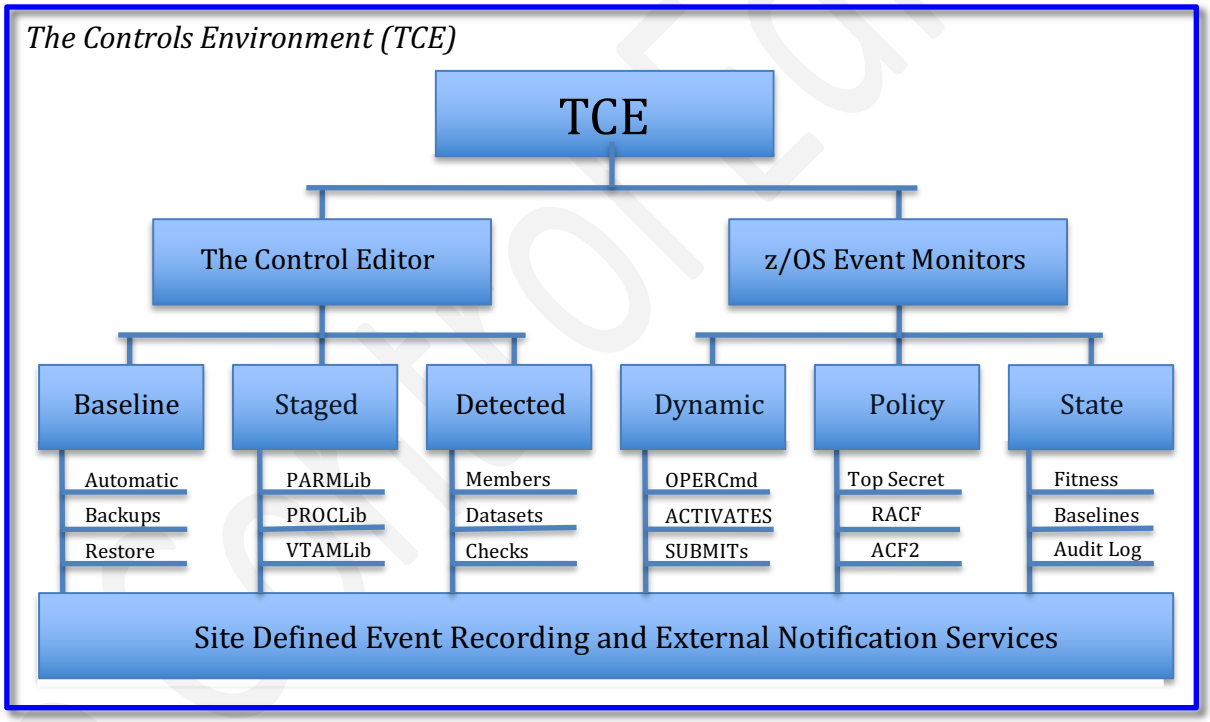
6 About The Control Editor (TCE)

The Control Editor, sometimes referred to as The Controls Environment (TCE) is a z/OS system change management tool that allows you to focus on the four possible classes of z/OS configuration change: Staged Changes, Dynamic Changes, Security Policy Changes and Changes in the State of the overall z/OS environment. It detects such changes in real-time, treating each as a unique change event recording it at varying levels of detail, as required by site policy, in a Control Journal and thereafter making it immediately available to a collection of interactive panels, reports, queries, batch processes and external notification services.

NewEra Software

z/OS Integrity and Compliance

z/OS Configuration Change Management and Change Event Notification - TCE



The Control Editor can be viewed as a "Compensating Control" providing a layer of non-invasive security over the z/OS configuration members housed in a defined set of partitioned datasets. TCE significantly enhances the level of security provided by an External Security Manager (ESM).

One way to envision the primary functions of The Control Editor is to think of it as a "Listener" on a z/OS subsystem interface that allows it to "Hear" all "Events", recording (Control Journal) only those that match a predetermined event profile (Control List) and optionally logging all defined events when forensic system analysis is required. These processes require no z/OS modifications, "Hooks" or "Exits" and are totally within the TCE Administrator's control.

The Control Editor is packaged with the Integrity Controls Environment (ICE) making its installation as simple as requesting the optional TCE license key from NewEra Technical Support. Environmental customization is accomplished by modifying default TCE configuration members.

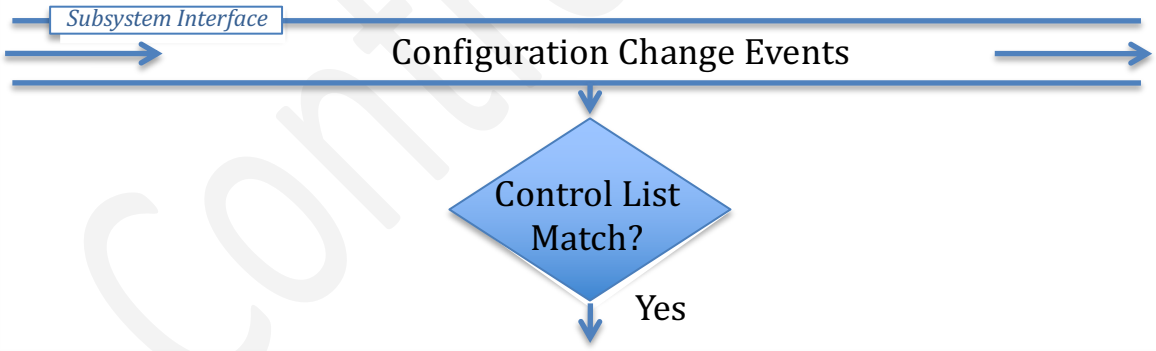
NewEra Software

z/OS Integrity and Compliance

z/OS Configuration Management and Auditing - The Control Editor

What is The Control Editor?

- ✓ One way to envision the primary functions of The Control Editor is to think of it as a "Listener" on a subsystem interface that allows it to "Hear" all "Events", recording only those that match a predetermined event profile (Control List) and optionally logging all defined events when forensic system analysis is required. These processes require no z/OS modifications, "Hooks" or "Exits" and are totally within the TCE Administrators control.



6.1 Types of Change Events

The Control Editor is used to manage and document four specific types of change events. Each of them and their sub-components are explained below.

6.1.1 Staged Changes

A Staged Change Event is any event that sets the baseline of a Controlled Dataset (BACKUP), changes the state of a Controlled Dataset (Edit, Rename, Delete, Add, Restore) or utilizes the content of a member in a Controlled Dataset (SUBMIT).

A Controlled Dataset, sometimes called a Boundary Dataset, is a dataset that is defined to the Integrity Controls Environment (ICE) during the installation of, or later dynamically, to The Control Editor. These Controlled Datasets contain Controlled Members, sometimes called Configuration Control Points.

Events that affect Controlled Datasets or indicate the use of Controlled Commands are captured and recorded in real-time in Control Journals. The grouping of possible event types is described below.

6.1.1.1 Dataset Backups

Full backups of defined Controlled Datasets are automatically taken and/or renewed at system startup (Backup Events) and stored in a discrete Control Journal called a “BACKUP” Journal. These stored copies and subsequent updates, stored in “PROCESS” Journals, represent the continuously updated configuration baselines from which configuration changes are identified and reported.

6.1.1.2 Member Edits

The editing of configuration members (Edit Events) that take place either using TSO under ICE or ISPF will optionally spawn the display of an event Descriptor Window. To proceed with the Edit Event, the requirements of the descriptor must be successfully completed, and the user must have UPDATE authority as determined by the External Security Manager (ESM). If the event is completed successfully, a copy of the member and the descriptor are stored. In addition, as with all Events, a summary record, called a META Record, containing “ISPF Like” statistics (META Data) is created and linked to the member and the descriptor. This META Data and associated links are accessed when TCE builds reports or answers ad hoc queries.

6.1.1.3 Member Renames

The renaming of configuration members (Rename Events) that takes place either using TSO under ICE or ISPF will optionally spawn the display of an event Descriptor Window. To proceed with the Rename Event, the requirements of the descriptor must be successfully completed, and the user must have UPDATE authority as determined by the External Security Manager (ESM). If the event is completed successfully, a copy of the member and the descriptor are stored.

6.1.1.4 Member Deletes

The deleting of configuration members (Delete Events) that take place either using TSO under ICE or ISPF will optionally spawn the display of an event Descriptor Window. To proceed with the Delete Event, the requirements of the descriptor must be successfully completed, and the user must have UPDATE authority as determined by the External Security Manager (ESM). If the event is completed successfully, a copy of the member and the descriptor are stored.

6.1.1.5 Member Adds

It is common practice for those who have the appropriate authority to do so, as determined by the External Security Manager (ESM), to add members to Controlled Datasets using ISPF 3.3 to copy an existing member into the Controlled Dataset under a new name. Such member additions (Add Events) are not captured or Journaled as they occur. Add Events are captured by invoking the Change Detection process either interactively or at specified intervals. When detected, the new member and its associated META Record are stored to the Control Journal creating a new Backup and Baseline.

6.1.1.6 Member Restores

Members stored in BACKUP or PROCESS Control Journals may be restored by a user with the appropriate authority as determined by the External Security Manager (ESM) by using the Restore Facility (Restore Event) provided within the Integrity Controls Environment. This process will optionally spawn the display of an event Descriptor Window. To proceed with the Restore Event, the requirements of the descriptor must be successfully completed. If the event is completed successfully, a copy of the member and the descriptor are stored.

6.1.1.7 SUBMIT

JCL stored in Controlled Datasets can be SUBMITTED directly from the command line during an edit session (SUBMIT Event) without External Security Manager (ESM) intervention. The attempt of such a submission will optionally spawn the display of an event Descriptor Window. To proceed with the SUBMIT Event, the requirements of the descriptor must be successfully completed. If the event is completed successfully, a copy of the member and the descriptor are stored.

6.1.1.8 Detected Changes

A "Detected Change" is a change to a member (a Control Point) that is housed in a Controlled Dataset (a Boundary Dataset) that was made using a process not managed by The Control Editor (Detected Change Event). Generally, such changes should be viewed as a violation of the operation policy inferred by an established Control Dataset List. When such events are detected, a copy of the member is stored. In addition, as with all Events, a summary record called a META Record containing "ISPF Like" statistics (META Data) is created and linked to the member. This META Data is accessed in the building of reports and answering queries.

6.1.2 Dynamic Change Events

The MVS Operator and Activate Command Sets are used to dynamically change the configuration or operation of the z/OS system environment. Generally, their use is limited to a select group of knowledgeable system operators and/or systems programmers.

6.1.2.1 Operator Commands

z/OS SET and MODIFY COMMANDS are used to dynamically alter the z/OS configuration (SET Events). The command strings calling such events, (SET PROG=01, SETPROG APF,add,dsnname=, MODIFY LLA) are captured as is the message text written to the system log as a result of the event. No Descriptor Window is displayed to alert the user that the event is being captured. In addition, as with all Events, a summary record called a META Record containing "ISPF Like" statistics (META Data) is created and linked to the messages. This META Data is accessed in the building of reports and answering queries.

6.1.2.2 ACTIVATE

IODF ACTIVATE COMMANDS are used to dynamically alter the I/O configuration (ACTIVATE Events). The command strings calling such events (ACTIVATE) are captured as is the message text written to the system log as a result of the event. No Descriptor Window is displayed to alert the user that the event is being captured. In addition, as with all Events, a summary record called a META Record containing "ISPF Like" statistics (META Data) is created and linked to the messages. This META Data is accessed in the building of reports and answering queries.

6.1.3 Security Policy Change Events

ESM specific commands may be detected, captured and recorded. No Descriptor Window is displayed to alert the user that the event is being captured. In addition, as with all Events, a summary record called a META Record containing "ISPF Like" statistics (META Data) is created and linked to the messages. This META Data is accessed in the building of reports and answering queries.

6.1.3.1 RACF

SETROPTS COMMANDS dynamically alter the RACF configuration (SETROPTS Events). The command strings calling such events, for example (SETROPTS PASSWORD(INTERVAL(30))) are captured as is the message text written to the system log as a result of the event.

6.1.3.2 Top Secret

Both the MVS Operator Command MODIFY TSS and the Top Secret specific command set TSS MODIFY are detected.

6.1.3.3 ACF2

The MVS Operator Command MODIFY ACF2 as well as the TSO ACF command Control GSO subcommands are detected.

6.1.4 Overall z/OS State Changes

An AuditLog is a summary of Inspection results and Changes detected within each defined Image within each defined Sysplex during an Image FOCUS Production Inspection (AuditLog Event). This highly summarized information is automatically posted to the Control Journals following each Inspection Cycle. Each posting contains links directly to the underlying Inspection Reports and Configuration Blueprint Packages. The Control

Editor History function uses these links to expand the information contained in the AuditLog into an articulating set of OSAudit Reports. In addition, as with all Events, a summary record called a META Record containing "ISPF Like" statistics (META Data) is created and linked to the AuditLog. This META Data is accessed in the building of reports and answering queries.

6.2 Control Journals

Control Journals are a set of sequential datasets that contain Control Dataset backups, directed and detected change events; related event META data, member and/or system log messages.

6.3 Change Event Notification

Event Notification is a process by which any user defined Edit, Operator and/or Policy Command can be reported in real-time via Email to an independently named set of recipients. Notification content: Event Identity, Event Descriptor/Command and Event Report may be customized for each individually defined notification event.

6.4 Panels, Reports and Queries

The Control Editor contains a broad array of panel displays, interactive worksheets, and reporting and query functions. In addition, all reports can be created and distributed in batch under the control of a site job scheduler or internal interval monitor. The remainder of this User Guide will explain these functions in detail.

6.5 JCL Validation

"TYPRUN=SCAN" has been available for the validation of JCL for a long, long time. It's considered a great way to pretest JCL prior to submission but unfortunately considered difficult to use. Inserting a new JOB CARD in the JCL Deck can be cumbersome, possibly leading to unintended JOB failures. TCE leverages JCL pretesting by automating the process by creating and submitting a conformed copy of the JCL, TYPRUN=SCAN is automatically inserted in the test deck before it is actually submitted. Validation results are returned immediately to the users Edit session, no need to try and track them down in the System Log.

6.6 TCE Terminology and Operational Components

Like all z/OS system management products The Control Editor (TCE) uses unique operational components and unique terminology to describe them. For a better understanding of these review the following sections of The Control Editor User Guide:

- Section 9 - Operational Sub-Systems, Task and Components
- Section 10 - Terminology

6.7 TCE Application Programming Interface

The Control Editor delivers an Application Programming Interface (API) that allows compliant REXX applications to directly query Event Records stored in The Control Journals. For a better understanding of the interface and sample applications, review the following section the Control Editor User Guide:

- Section 11 – The Control Journal API

7 Index

T

W

NewEra Software, Inc.

Mailing Address:

18625 Sutter Blvd, Suite 950
Morgan Hill, CA 95037

Phone:

(408) 520-7100
(800) 421-5035

Text:

(669) 888-5061

FAX:

(408) 413-2800
(866) 939-7099

Email Address:

support@newera.com

Web Site:

http://www.newera.com

Technical Support:

24 hours a day, 7 days a week
1-800-421-5035
support@newera.com