ATTACHMENT 71111.13

INSPECTABLE AREA: Maintenance Risk Assessments and Emergent Work Control

CORNERSTONES: Initiating Events (20%)
Mitigating Systems (70%)
Barrier Integrity (10%)

INSPECTION BASES: Paragraph (a)(4) of 10 CFR 50.65, the Maintenance Rule (MR), requires licensees to assess and manage plant risk related to maintenance activities during all modes of plant operation. Risk is assessed and managed for both scheduled maintenance and emergent work. Risk management minimizes risk-significant configurations and initiating events and maximizes availability of mitigating systems and barriers to radiological releases.

LEVEL OF EFFORT: Sample maintenance activities before commencement, in progress, or completed, as available each calendar quarter. The goal is to inspect 15 to 25, 20 to 30, and 25 to 35 maintenance activities including emergent work control activities in a year at 1-unit, 2-unit, and 3-unit sites respectively. The inspectors should include a mixture of scheduled and emergent work in selecting samples. Samples should take into account the relative plant risk and the prevalent type of work activities at the site. Although the number of required samples is an annual goal, available work activities should be inspected each quarter to ensure a reasonable distribution throughout the year. It is intended that (a)(4) inspection be integrated as much as practicable with other routine monitoring of plant activities and configuration. The final sample selected for review should not include maintenance activities that screened out at Block 5 of Appendix A of this procedure.

71111.13-01 INSPECTION OBJECTIVES

01.01 Verification of performance of assessments of plant risk related to planned or emergent maintenance activities during all modes of plant operation when and as required by 10 CFR 50.65(a)(4) and licensee procedures.

01.02 Verification of adequacy of risk assessments (RAs), limited for this Inspection Procedure (IP), to accuracy and completeness of information considered in the RA and appropriate use of the RA tool or process.

01.03 Verification of management of resultant risk, including, as applicable, entry into appropriate licensee-established risk categories or bands, effective implementation of normal work controls or risk management actions (RMAs) in accordance with licensee procedures, and preservation of key safety functions.

01.04 Verification of effective planning and controlling of emergent work activities resulting from unforseen situations, including prompt reassessment of the resultant plant risk and effective management of that risk.

01.05 Verification of identification and resolution of problems associated with the licensee's implementation of 10 CFR 50.65(a)(4) and emergent work control.

71111.13-02 INSPECTION REQUIREMENTS

02.01 Risk Assessment and Management of Risk

a. Risk Assessment Performance. Verify performance of RAs when required by §50.65(a)(4) and in accordance with licensee procedures, prior to changes in plant configuration for maintenance activities, including preventive maintenance, surveillance and testing, (and promptly for emergent work) during all modes of plant operation. Verify RA performance for configuration changes involving structures, systems, or components (SSCs) within the scope of the MR or the licensee-established limited RA scope allowed by §50.65(a)(4) with emphasis on higher-safety/risk-significant configurations. For emergent work, verify that the licensee performs the RA (to the extent practicable and commensurate with safety) before changing the plant configuration further, but in any case, promptly and to the extent practicable concurrently with, but without delaying, plant stabilization and restoration.

b. Risk Assessment Adequacy. Verify the accuracy and completeness of the information considered in the RA. Verify the appropriate use of the licensee's RA tool, i.e., that the licensee uses it a manner consistent with (1) its capabilities and limitations, (2) plant conditions and evolutions, (3) external events and containment status, and (4) licensee procedures. Engage the licensee when necessary to have inadequate RAs promptly and correctly re-performed. For completed work for which the normal plant configuration has been restored, an omitted (or inadequate) RA may still need to be performed (or re-performed correctly) by the licensee (or the configuration in question evaluated independently by the NRC if possible) in order to determine the associated change in plant risk for significance determination purposes.

c. Risk Management. Verify that the licensee recognizes, and/or enters as applicable, the appropriate licensee-established risk category or band according to RA results and licensee procedures. Verify that normal work controls or risk management actions (RMAs) as required are promptly and effectively implemented commensurate with the risk band in effect and in accordance with licensee procedures. Verify that the key safety functions for the plant mode of operation are preserved. Re-verify implementation of RMAs (or different RMAs) that may now be required by licensee procedures following performance (or re-performance) of previously omitted (or inadequate) RAs.

02.02 Emergent Work Control

a. During emergent work (combined with scheduled work in progress or alone), verify that the licensee takes actions to minimize the probability of initiating events, maintain the functional capability of mitigating systems and maintain barrier integrity.

b. Review emergent work-related activities such as troubleshooting, work planning and scheduling, establishing plant conditions and aligning equipment, tagging (clearances), temporary modifications and equipment restoration to ensure that the plant is not placed in an unacceptable configuration (including violation of Technical Specifications).

02.03 Problem Identification and Resolution. Verify that the licensee is identifying problems with maintenance-related risk assessment and management and emergent work control and entering them in the corrective action program. For a sample of significant problems documented in the corrective action program, verify that the licensee has identified and implemented appropriate corrective actions. See Inspection Procedure 71152, “Identification and Resolution of Problems,” for additional guidance.

71111.13-03 INSPECTION GUIDANCE

03.01 Risk Assessment and Management of Risk

General Guidance

This inspection is intended to be performance based and risk informed. It is expected to be initiated only in response to plant configuration changes associated with actual scheduled and emergent maintenance activities, including ones that are planned, in progress, or have been completed. Emphasis should be on the higher risk-significant configurations/SSCs. It is not the intent of this procedure to perform a programmatic review of the licensee’s §50.65(a)(4) program or to address those instances in which plant configuration is changed for non-maintenance purposes. In-depth examination of (1) the limited scope or the risk-informed evaluation process used to develop it, (2) the licensee’s RA tool(s) or process(es) themselves, and (3) licensee risk bands or categories and RMAs is reserved for supplemental inspection by regional and/or headquarters inspectors and senior reactor analysts (SRAs) under IP 62709,“Configuration Risk Assessment and Risk Management Process.”

To the extent practicable, the inspection activities prescribed by this IP should be integrated with the resident inspector’s routine monitoring of plant activities and configuration.

The plant configuration changes to be inspected are those involving SSCs within the scope of the maintenance rule (or the limited scope as allowed by 10 CFR 50.65(a)(4)) and certain other risk-significant SSCs (See the note at the text for Block 7 in Appendix A of this procedure).

The significance of findings resulting from performance of this IP will be determined with the Reactor Safety Significance Determination Process (SDP) of NRC Inspection Manual Chapter 0609. The need for supplemental inspection will be determined on the basis of the requisite non-green findings in accordance with the NRC Reactor Oversight Program (ROP). Use of the Reactor Safety SDP for §50.65(a)(4) findings subsumes defining "planned maintenance" as scheduled or emergent, but properly risk-assessed and risk-managed in accordance with (a)(4).

Before performing this procedure, the inspector should develop an understanding of the licensee's program for conducting risk assessments and managing the resultant risk and become familiar with the associated procedures. Note that while it is not within the scope of this inspection to perform a programmatic review of the licensee’s (a)(4) procedures, it would be appropriate to question and bring to the licensee’s attention anything in the procedures discovered in the course of this familiarization that is not clear or appears to be incorrect.

03.02 Emergent Work Control

General Guidance

It is not within the scope of this inspection procedure to routinely observe maintenance activities. However, for emergent work activities, inspectors should verify that the licensee is following the work schedule and work plan, and has taken precautions to preclude affecting adjacent SSCs.

Observe equipment lineups and tagging when potential errors could affect other operating systems. When appropriate, verify that redundant components are maintained in an operable status. See Baseline Inspection Procedure 71111.04, "Equipment Alignment," for additional guidance.

The inspector should consider if potential maintenance errors could initiate an event or affect defense-in-depth when selecting work activities to review. The review should be limited to emergent work activities that could cause an initiating event to occur or affect the functional capability of mitigating systems and barrier integrity. Refer to the guidance in the table below for selecting inspection activities. The RA and risk management actions associated with emergent work will be inspected in accordance with Appendix A.

Cornerstone	Inspection Objective	Risk Priority	Example
Initiating Events	Identify emergent work that could cause initiating event(s)	Troubleshooting not well defined by implementing procedure Work near SSCs able to cause transients with higher risk than reactor trip	Troubleshooting electrical equipment associated with or adjacent to safety injection initiation circuits
Mitigating Systems	Identify mitigating systems, credited by licensee as operable, that are impacted by emergent work planning or performance	Emergent work when high-risk configurations already exist due to planned, on-line maintenance Emergent work on support systems that may affect multiple SSCs	Emergent repair of room cooling equipment with other mitigating SSCs already out of service
Barrier Integrity	Identify Barrier systems, credited by licensee as operable, that are impacted by emergent work planning or performance	Emergent work when high-risk configurations already exist due to planned, on-line maintenance	Emergent work on containment purge valves, containment isolation valves and personnel air lock

Specific Guidance

03.01 Risk Assessment and Management of Risk. See Appendix A.

03.02 Emergent Work Control. No specific guidance is provided in this procedure.

03.03 Identification and Resolution of Problems. No specific guidance is provided in this procedure.

71111.13-04 RESOURCE ESTIMATE

The annual resource expenditure for this inspection procedure is estimated to be 92 to 124 hours for sites with one reactor unit; 102 to 138 hours for sites with two reactor units; and 123 to 165 hours for sites with three reactor units.

71111.13-05 COMPLETION STATUS

Inspection of the minimum sample size will constitute completion of this procedure in the Reactor Programs Systems (RPS). That minimum sample size will consist of inspecting 15, 20, and 25 maintenance activities including emergent work control activities in a year at 1-unit, 2-unit, and 3-unit sites respectively.

71111.13-06 REFERENCES

Section 50.65 of Part 50 of Title 10 of the *Code of Federal Regulations* (10 CFR 50.65), "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants"

Regulatory Guide 1.160, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants"

Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants"

Regulatory Guide 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests and Experiments," November 2000

The Nuclear Energy Institute's (NEI's), NUMARC 91-06, "Industry Guideline for Shutdown Operations"

NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants"

Revised Section 11, dated February 22, 2000, “Assessment of Risk Resulting from Performance of Maintenance Activities,” of NUMARC 93-01

NEI 96-07, Revision 1, "Guidelines for 10 CFR 50.59 Implementation,"November 2000

Inspection Procedure 71111.04, "Equipment Alignment"

Inspection Procedure 71111.19, "Post Maintenance Testing"

Inspection Procedure 71111.20, "Refueling and Outage Activities"

Inspection Procedure 71152, "Identification and Resolution of Problems"

Supplemental Inspection Procedure 62709, "Configuration Risk Assessment and Risk Management Process"

NRC Inspection Manual Chapter 0609, "Significance Determination Process"

NRC Inspection Manual Chapter 2515, Appendix D, "Plant Status Review"

NRC Information Notice 2000-13, "Review of Refueling Outage Risk," dated September 27, 2000

END

The attached flow chart delineates the structure, logic, and process flow for inspection of licensee activities related to 10 CFR 50.65(a)(4). The flow chart guides the inspector in (1) verifying that risk assessments (RAs) are performed when required (RA Performance Verification Phase); (2) verifying that RAs are adequate (RA Adequacy Verification Phase); (3) verifying that the appropriate licensee risk bands are entered based on the RAs; (4) verifying that normal work controls or risk management actions (RMAs), consistent with those risk bands, are promptly and effectively implemented in accordance with licensee procedures; and (5) verifying that the key safety functions are preserved by those RMAs (Risk Management Verification Phase).

Each flowchart block is numbered to help the inspector compare the flowchart to the specific written guidance. Also, each flowchart block section in the text of this appendix references the pertinent paragraph(s) in the revised Section 11 of NUMARC 93-01.

At certain junctures in the inspection process, if the inspector identifies licensee performance issues including omitted, but required RAs, inadequate RAs, unrecognized risk, unimplemented or ineffectively implemented RMAs, the flowchart provides for licensee engagement for safety and regulatory review for risk evaluation and preliminary enforcement evaluation in Block 9.

RA PERFORMANCE VERIFICATION PHASE

Block 1 (Start) - Configuration Change (11.3)

ENTRY CONDITION: Based on the knowledge gained through plant status review (Manual Chapter (MC) 2515, Appendix D), including routine walkdowns and routine monitoring of maintenance activities planned and in progress, the inspector should enter this inspection procedure when there has been (or will be) a change in plant configuration that resulted (or could result) in an actual (or potential) increase in plant risk.

Block 2 – Is the Configuration Change Related to Maintenance Activity? (11.3)

Is the configuration change related to maintenance activity (scheduled or emergent) during any mode of plant operation that is not yet started, in progress, or completed? Maintenance activities include, but are not limited to, surveillance, post-maintenance testing, and corrective and preventive maintenance. If so, proceed to Block 3. If not, proceed to Block 5 and stop the inspection process for this particular configuration change.

Block 3 - Is More than One SSC Out-of-Service? (11.3.4)

Determine if the planned, ongoing, or completed maintenance activity and associated system lineups affect more than one SSC within the full scope of SSCs covered by 10 CFR 50.65(b) or the limited scope allowed by §50.65(a)(4), taking into account any other out-of-service and potentially risk-significant SSCs in the entire unit/plant. For example, an SSC may be taken out of service coincident with other maintenance activities, but they do not disable another (additional) SSC or in any other way increase plant risk. Nevertheless, even if the SSC being considered is or will be the only potentially risk-significant SSC out of service in the plant, proceed to Block 4 for other relevant considerations. If the configuration change being considered involves more than one potentially risk-significant SSC, proceed directly to Block 6.

Removal from service of a single SSC is normally adequately covered by Technical Specifications (TS). Stopping the inspection process based on only one SSC being out of service (in the entire unit, not just for the maintenance-related configuration being

considered), should occur very infrequently because plant configuration changes associated with maintenance activities normally affect additional SSCs that are out of their normal plant configuration for various reasons.

Block 4 - Inspection May Continue With Only One SSC Out of Service (11.3.4)

At the inspector's discretion, when conditions warrant, even with only one SSC out of service, the inspection may continue. Such conditions include (but are not limited to) external events such as severe weather, plant conditions or evolutions such as governed by AOPs, and surveillance or test activities that may increase the likelihood of a transient or the ability to cope with an event with important mitigation equipment out of service. An important example is taking standby AC power sources out of service when conditions such as severe weather or switchyard maintenance exist, or are expected, that could increase the probability of loss of offsite power. Note that various conditions, including temporary modifications or severe weather, may also impact the ability or availability of plant personnel to perform important recovery actions. If the decision is to continue the inspection, proceed to Block 6. If not, proceed to Block 5 and stop the inspection process for this particular configuration change.

Block 5 - Stop Inspection Process

EXIT CONDITIONS: The plant configuration change being considered is not associated with maintenance (Block 2), or affected SSCs are not within the MR full or (a)(4) limited scope and are not risk significant (Block 3); or there is only one risk-significant SSC out of service with no other relevant considerations (Block 4); or no risk assessment was required (Block 7). Hence, further inspection under this IP is not expected for the configuration change being considered.

Note that when a maintenance activity screens out in this manner it should not be counted as a valid sample in fulfilling the inspection goals given under "Level of Effort" at the beginning of this procedure. The inspector may need to use the criteria in this portion of the procedure to screen several maintenance activities in order to obtain a valid sample, i.e., one in which licensee (a)(4) activities are required and may be followed to conclusion.

Block 6 - Did the Licensee Perform a Risk Assessment (RA) (11.3)?

Determine if the licensee performed an RA for the maintenance activity and associated configuration change being considered, whether planned, ongoing or completed. If not, continue to Block 7. If yes, proceed to Block 8.

Block 7 - Was a Risk Assessment (RA) Required? (11.3.3)

If no RA was performed, use the guidance below to determine if an RA was actually required and when. If the inspector believes an RA was required, proceed to Block 9 for regulatory review. If no RA was required, proceed to Block 5 and stop the inspection process for this particular configuration change.

Determine if an RA was required using the following criteria:

1. When Required. RAs are required by (a)(4) prior to maintenance-related plant configuration changes and are normally performed for scheduled maintenance. However, emergent conditions, such as external events or SSC failures or degraded performance in service or during testing, may require actions prior to performing an RA, or could invalidate the existing RA. In this case, the RA should be performed (or reevaluated) to address the changed plant conditions. The industry guidance, revised Section 11 of NUMARC 93-01, as endorsed by RG 1.182, states that if the plant configuration is restored prior to conducting or

reevaluating the RA, the RA need not be conducted, or reevaluated if already performed. Nevertheless, to the extent practicable and commensurate with safety, the licensee should perform or reevaluate the RA before changing the plant configuration further, but in any case, promptly and to the extent practicable concurrently with, but without delaying, plant stabilization and restoration. Note that licensee deviation from work schedules and work plans, just as emergent work can, may invalidate risk assessments prepared for the maintenance period (e.g., the common 12-week rolling schedule).

2. Operating Modes When RA Required. RAs are required by (a)(4) for maintenance activities performed during all modes of plant operation and transitions between modes. For (a)(4) purposes, at power means normal steaming (Mode 1) and startup (Mode 2). Shutdown means hot standby (Mode 3 in a pressurized water reactor (PWR) only), hot shutdown (Mode 3 in a boiling water reactor, Mode 4-PWR), cold shutdown (Mode 5), and refueling (Mode 6). Plants without a shutdown probabilistic risk assessment (PRA) must still assess shutdown maintenance risk by some means, typically an expert panel using a qualitative (key safety function) or blended qualitative/quantitative approach. However, for a BWR in hot shutdown (Mode 3) with reactor coolant system (RCS) temperature above 200°F, or for a PWR in hot standby (Mode 4) between normal operating temperature (NOT) and 350°F, RCS heat removal normally requires portions of the steam, feed, auxiliary feed, and condensate systems (and support systems) to be operating. RA tools based on at-power PRA should be used under these conditions. See the detailed explanation under Block 8.

3. RA Scope. RAs are required by 10 CFR 50.65(a)(4) for maintenance activities involving SSCs within the scope of the MR as defined by §50.65(b). However, (a)(4) allows the scope of the SSCs to be addressed by RAs to be limited to those that a risk-informed evaluation process has shown to be significant to public health and safety.

If industry guidance is followed, RA scope will include, as a minimum, high-safety/risk-significant (HSS) in-scope SSCs (as determined by an expert panel), plus SSCs included in the scope of the plant's level 1, internal events PRA. Therefore, when evaluating whether an RA was required, inspectors may need to consider certain other risk-significant SSCs that may not be within the scope of the MR. This may also be necessary later when determining RA adequacy in terms of input information accuracy and completeness.

NOTE: Certain SSCs, which for various reasons are not included in the normal scope of the maintenance rule as defined by §50.65(b) (e.g., those that are used in the Abnormal Operating Procedures (AOPs)), may become risk significant during shutdown or under other conditions modeled (or not) in the plant's PRA. Should the licensee fail to consider such SSCs in its risk assessments, ensure that the licensee has an adequate technical basis for the exclusion consistent with the intent of NRC-endorsed industry guidance. It may be necessary for the licensee's expert panel to assess the risk associated with these SSCs qualitatively. It would also be appropriate for inspectors to consider these SSCs in evaluating the adequacy of risk assessments. However, it is recognized that although the licensee's failure to consider them could result in a risk-significant finding, it would not, in itself, constitute a violation of 10 CFR 50.65(a)(4) under the current enforcement guidance.

The resident staff is not expected to verify RA tools or process validity itself. This is reserved for supplemental inspection if necessary. RA adequacy verification for purposes of this IP is limited to verifying that the RA input information was accurate and complete and that the tool was used appropriately. RA input information is first verified by evaluating the fidelity of the RA to the actual plant configuration under Block 8. Blocks 10 and 11 then verify preservation of key safety functions during shutdown and at power, respectively. Finally, Block 14 verifies consideration of external events, internal flooding, and containment if applicable. Appropriate RA tool use is verified under Block 13. Deficiencies are addressed in Block 9.

Block 8 - Does Assessed Configuration Match Actual Plant Configuration? (11.3)
Based on knowledge of current plant conditions, obtained, for example, through walkdowns while performing MC 2515, Appendix D, and/or IP 71111.04, “Equipment Alignment,” verify that actual plant configuration matches the RA configuration. Using the guidance below, emphasis should be placed on the more safety/risk-significant SSCs. Inspectors should pay particular attention to SSCs that are degraded but operable. This should include a review of compensatory actions to determine applicability for the current plant conditions. If actual configuration matches the RA, proceed to Block 10 if the plant is shut down or Block 11 if it is at power. If there is a mismatch, proceed to Block 9. The references listed below may be helpful in making this determination.

It may be possible to perform this review in conjunction with routine monitoring of plant status, work planning, ongoing work, etc., and also as part of the review of effective implementation of risk management actions such as verifying that redundant (backup) components are maintained in an operable status. Note that deviations from maintenance schedules may invalidate the RA in effect.

Other RA input information should include (but is not limited to) mode of operation; concurrent plant conditions and evolutions, temporary alternations or modifications (particularly those that could inhibit important operator actions), or other maintenance activities planned or in progress with increased probability of initiating events or degradation of mitigating systems; containment status; and external events (expected, imminent, or in progress).

The risks of initiating events or degradation of mitigating systems from specific maintenance errors are not typically included in PRA studies. Therefore, the RA should also consider qualitatively whether potential maintenance errors could initiate an event, affect the defense-in-depth principle, affect the functional capability of mitigating systems, or degrade barrier integrity (key safety functions).

Plant Configuration References:

a. SDP Notebook. Drawing upon PRA insights and developed specifically for the plant, the SDP Notebook is intended as an aid to using SDP worksheets. Although not its primary function, the SDP Notebook lists front-line equipment needed to mitigate initiating events, support equipment and important operator recovery actions (which may be inhibited by the configuration change being considered, particularly temporary modifications). The SDP Notebook also contains the plant-specific SDP work sheets which list full creditable mitigating capabilities for each safety function.

b. Emergency Operating Procedure (EOP) Functional Restoration Guides. Useful in determining equipment necessary for support of key safety functions (called "critical safety functions" in the guides). At power, they are containment integrity (isolation, pressure and temperature control), reactivity control, reactor coolant

system (RCS) heat removal, and RCS inventory control. Shutdown key safety functions are decay heat removal, inventory control, power availability, reactivity control, and containment.

c. Technical Specifications (TS) and their bases

d. MC 0609, Appendix G (shutdown) and Appendix H (containment)

e. NRC Information Notice 2000-13, "Review of Refueling Outage Risk"

The RA for the existing operating mode may require PRA that is not nominally consistent with that mode. For example, when the reactor is shutdown but the reactor coolant system temperature and pressure are above residual heat removal (RHR) entry conditions, certain normal steaming SSCs (e.g., parts of the steam, feed, and condensate systems) are needed to remove decay heat. Initiating events that could impact core cooling are similar to those considered in full-power PRAs (e.g., loss-of-coolant accidents, loss of feedwater, loss of support systems, loss of offsite power). Mitigating systems required would be among those required at power, particularly those required by TS, except for certain containment systems. Therefore, under these conditions, unless the licensee's PRA and/or risk assessment tool models such transitional conditions, at-power PRA analyses may need to be used.

Should full-power (and typically only Level 1) PRA analyses be used for shutdown, the RA should consider that (1) certain systems require manual operation if their automatic initiation is blocked (e.g., automatic initiation of safety injection (SI) in a PWR is blocked during hot shutdown unless "High" or "High High" containment pressure occurs), and (2) certain containment conditions may not be required to be limited (e.g., atmospheric oxygen concentration) or certain containment systems may not be required to be operable (e.g., BWR drywell cooling fans or hydrogen igniters and mixing systems in ice condenser containments). Thus, for example, the susceptibility to hydrogen burns following a severe accident may be greater than at full power. However, decay heat will be much less than heat at power, allowing more time for operator recovery.

Block 9 - Licensee Engagement and Regulatory Review

For required but omitted RAs (from Block 7), question the licensee about the omission (licensee engagement). If the licensee cannot demonstrate that an RA was not required, this is a licensee performance issue that needs to be reviewed in accordance with MC 0612 (formerly 0610*), Appendix B. Failure to perform a required RA is a potential violation of 10 CFR 50.65(a)(4) per the current enforcement guidance.

For RAs that the inspector believes are inadequate (from Blocks 8 and 10 through 14), question the licensee about the deficiencies in the accuracy and completeness of the input information (e.g., a potentially risk-significant mismatch between the assessed and actual plant configurations from Block 8 or loss of key safety functions from Blocks 10 or 11), or about inappropriate use of the RA tool or process (e.g., inconsistent with its capabilities and limitations, plant conditions, licensee procedures from Block 13). If the licensee cannot demonstrate RA adequacy, this is a licensee performance issue that needs to be reviewed in accordance with MC 0612, Appendix B. Failure to perform an adequate RA is a potential violation of 10 CFR50.65(a)(4) per the enforcement guidance.

For prescribed RMAs not implemented, or implemented ineffectively (from Blocks 16 and 17), question the licensee about the deficiencies (e.g., SSCs relied upon for backup being worked on, operators not aware of risk-significant maintenance activities, etc.). If the licensee cannot demonstrate that the omitted RMAs are not required or that RMAs are effectively implemented, this is a licensee performance issue that needs to be reviewed

in accordance with MC 0612, Appendix B. Failure to manage risk is a potential violation of 10 CFR 50.65(a)(4).

The resident may encounter situations in which (1) there is or will be a potentially high-risk configuration of the plant that the licensee is not aware of because it was not risk-assessed when required, and hence, risk management actions are not initiated, (2) a risk assessment was done incorrectly and may have substantially underestimated the risk, hence also resulting in not initiating proper risk management actions, and/or (3) the licensee failed to effectively implement its own prescribed risk management actions even if the risk was correctly assessed. Under these circumstances, the plant may remain in a high-risk configuration, even though an event may not result.

Unless risk can be independently assessed by the NRC (not presently possible) the licensee needs to do so, not only to comply with 10 CFR 50.65(a)(4), but also in order to determine the significance of the licensee's failure to perform the risk assessment in the first place, or likewise, to re-perform the risk assessment correctly to gage the risk significance of the original underestimated risk.

The inspector is not expected to try to force the licensee to comply with the regulation. However, pointing out or at least questioning apparent performance deficiencies (i.e., licensee engagement) may be necessary in order to prompt the licensee to consider the proper action commensurate with the risk significance of the issue when made aware of the circumstances. Note that updated or corrected risk assessment results are needed to continue the inspection process.

If the licensee fails to take appropriate action after being informed of the issue or cannot demonstrate why such action is not necessary, the inspector should consult with regional and/or headquarters staff as listed below. Evaluate the adequacy of corrected/updated RAs as described in Blocks 8 and 10 through 14.

Continue regulatory review as described below for preliminary determination of the significance of the issues and address the potential enforcement issues. At the discretion of the inspector, determine the significance of the issues at each juncture in the process at which they are first identified or review the issues when convenient and as described at the end of the inspection process at Block 18. Block 18 prescribes screening the issues through Appendix B of MC 0612. To the extent practicable, continue inspection concurrently with regulatory review. Inspectors should use Figure 1 and Group 1, 2, and 3 questions in Appendix B of MC 0612 in determining if an issue should be documented in an inspection report as a finding.

After discussion among the inspection staff and addressing the issues with the licensee, regulatory review may involve consulting as necessary with supervision and other cognizant regional and headquarters personnel including the following:

1. Regional Division of Reactor Safety (DRS) staff, and headquarters staff of the Quality Assurance, Vendor Inspection, Maintenance and Allegation Branch (IQMB) for MR questions

2. Office of Nuclear Reactor Regulation (NRR) and regional reactor analysts and senior reactor analysts (SRAs) for risk issues. The results of initial and updated RAs should be available, before contacting the SRA.

3. Regional and headquarters enforcement staff and IQMB for enforcement questions

Block 10 - Are Shutdown Key Safety Functions Maintained? (11.3.6.1)

Although the actual configuration matches the assessed configuration, minimum key safety functions may not have been adequately preserved or maintained. The SSCs addressed by a shutdown RA should include those necessary to support the shutdown key safety functions which are (1) decay heat removal capability, (2) RCS inventory control, (3) electric power availability, (4) reactivity control, and (5) containment (primary/secondary). See NUMARC 91-06 for further guidance.

MC 0609, Appendix G, lists SSCs needed to maintain minimum shutdown key safety functions. The lists are categorized according to the shutdown condition of the plant. These SSCs constitute a minimum acceptable threshold. Using MC 0609, Appendix G, verify that the licensee has maintained minimum shutdown key safety functions. If so, proceed to Block 12. If not, proceed to Block 9.

NOTE: To expedite an outage, the license may voluntarily enter TS limiting conditions for operation (LCOs) by removing certain SSCs from service while still in hot standby or hot shutdown in anticipation of entering cold shutdown before the LCOs expire and TSs would be violated. Under these circumstances, even if not yet in violation of TS requirements, the plant risk may be higher than indicated by the RA.

Block 11 - Power Operations - Key Safety Functions Maintained? (11.3.4)

Although the actual configuration matches the assessed configuration, minimum key safety functions may not have been adequately preserved or maintained. The SSCs addressed by an at-power RA should include those necessary to support the at-power key safety functions. For power operation, key plant safety functions are those that ensure (a) the capability to maintain integrity of the RCS pressure boundary, (b) the capability to shut down the reactor and maintain it in a safe shutdown condition, and (c) the capability to prevent or mitigate the consequences of accidents that could result offsite release of radioactivity in excess of 10 CFR Part 100 guidelines. Examples of at-power key safety functions are (1) containment integrity (isolation, pressure and temperature control), (2) RCS inventory control, (3) RCS heat removal, and (4) reactivity control.

The site-specific SDP notebook tabulates the most risk-significant front-line and support systems and major components and also lists important operator recovery actions (some of which may be inhibited by the maintenance activity being considered, particularly temporary modifications). In addition, the success criteria on the reactor safety SDP work sheets (MC 0609, Appendix A) can be used to help evaluate the preservation of each at-power key safety function. Using this information as an aid, verify that the licensee has maintained at-power key safety functions. If so, proceed to Block 12. If not, proceed to Block 9.

Block 12 - Did the Licensee Enter the Appropriate Risk Category? (11.3.4)

Using the licensee procedures and processes that govern maintenance risk assessment and management at power or shut down, determine which licensee-established risk category or band is prescribed for the risk level obtained from the RA. Verify that the licensee has recognized this risk level and entered the appropriate category. If the licensee entered the appropriate risk category, proceed to Block 13. If not, proceed to Block 9.

Note that the parameter(s) by which the licensee defines its risk categories or bands and/or the risk levels at which RMAs are prescribed may differ from the industry guidance. In addition, different risk metrics may be employed for different plant conditions or the capability of the RA tool(s). For example, some licensees define their risk bands in terms of incremental (conditional) core damage probability (ICDP). Others may use core damage

frequency (CDF). For those plants with Level II PRAs, large early release frequency (LERF) may be used while at power. For shutdown, time to boil may be considered. While not expected to challenge the licensee's system, at least not initially, the inspector should understand the relationship of the particular licensee's risk bands to those prescribed in the industry guidance for (a)(4), revised Section 11 of NUMARC 93-01, as endorsed by RG 1.182.

If the licensee uses CDF and defines risk bands, for example, in terms of multiples of the plants base CDF, the licensee risk bands can be related to the risk metric used in the industry guidance, ICDP, by the following equation:

ICDP = ΔCDF(outage time [in hours]/8760 hours/reactor year)

If for example, a licensee used CDF, but did not establish specific time limits for maintenance activities, the inspector could calculate how long it would take at a given instantaneous CDF (assuming it were maintained for the entire year), compared to the baseline risk, or ΔCDF, to exceed the Section 11 threshold of 1.0×10^{-6} ICDP, at which level Section 11 calls for RMAs to be initiated. This is done by setting ICDP equal to $1.0\ 10^{-6}$, entering the existing ΔCDF, and solving for the outage time. That is, time to exceed 1.0×10^{-6} ICDP = $(8760 \times 10^{-6})/\Delta CDF$. This information can aid the inspector in evaluating the need for or effectiveness of the licensee's RMAs. It would be appropriate for the inspector at least to question the licensee about maintenance risk that is allowed to exist long enough for ICDP to exceed 1.0×10^{-6}, particularly without time limits and if the licensee's procedures do not call for the initiation of RMAs while in their existing risk band.

Block 13 - Was the RA Tool Used Appropriately? (11.3.4)

This block is the second part of RA adequacy verification, i.e., verifying appropriate use of the RA tool or process. For purposes of this IP, appropriate use means that the RA tool or process is used in a manner consistent with (1) its capabilities and limitations, (2) plant conditions and evolutions, (3) external events and containment status, and (4) licensee procedures.

Using licensee procedures that control the RA tools or processes for power operations, determine whether a qualitative or a quantitative method is used for at-power RAs and shutdown RAs. Qualitative RAs typically addresses the impact of the maintenance activity upon key safety functions and are often performed by an MR expert panel. Quantitative RAs use a tool or method that considers PRA insights (e.g, matrices, on-line safety monitors, etc.).

After becoming familiar with the capabilities and limitations of the licensee's RA tool(s) or process(es) and with the associated procedures, the inspector should be alert to the application of the tool beyond its capabilities. For example, work plans that allow more SSCs to be out of service than the risk tool is capable of assessing with adequate fidelity should be questioned. No more than two SSCs should be out of service if using a 2x2 matrix. Question more than four or five SSCs out of service if a cutset editor tool was used because their fidelity degrades with more than four or five inputs. Consult Supplemental Inspection Procedure 62709, "Configuration Risk Assessment and Risk Management Process," for more information on RA tool capabilities and limitations.

When satisfied that RA input information was accurate and complete and that the RA tool or process was used appropriately, RA adequacy is verified; so proceed to Block 14. If not, the RA may not have been adequate; proceed to Block 9.

Block 14 - Did the RA Consider Containment Integrity, External Events and Internal Flooding and Should They Have Been Considered? (11.3.4)

Actual, forecasted, or potential external events, internal flooding, or containment integrity degradation may not have been addressable by a PRA-based risk tool with limited capabilities. However, if during the maintenance activity, introduction of external events, internal flooding, or containment integrity degradation exist or are expected, they should have been addressed by some means such as qualitatively by an expert panel. Using the guidance below, verify that in addition to addressing plant conditions during the maintenance activity in question, the RA addressed these considerations. If so, proceed to Block 15. If not, the RA may have been inadequate; proceed to Block 9.

Containment. The RA may need to consider circumstances which could affect the ability of the containment to perform its function as a fission product barrier. These would include (1) whether new containment bypass conditions are created, or the probability of containment bypass conditions is increased; (2) whether new containment penetration failures that can lead to loss of containment isolation are created; and (3) if maintenance is performed on SSCs of the containment heat removal system (or SSCs upon which this function is dependent), whether redundant containment heat removal trains should be available.

External Events. The RA should consider external events such as weather or fire if such conditions are imminent or likely or have a high probability of affecting the plant during the planned out-of-service duration. Certain configuration changes, or maintenance activities, particularly those involving temporary modifications (e.g., long-term removal of exterior doors, hazard barriers, or floor plugs), can increase the likelihood of external events or increase the severity of their effects. For example, fire within the plant (considered an external event) may be a significant risk contributor due to plant design, and the nature of the work may increase the risk of starting a fire (e.g. hot work). External events also include problems with the electric power grid or other circumstances (e.g., severe weather, brush/forest fires) that could cause a loss of offsite power.

Internal Flooding. Internal flooding (from internal or external sources) should be addressed if pertinent. The RA should consider the potential for maintenance activities to cause internal flood hazards and for maintenance activities to expose SSCs to flood hazards in a manner that degrades their capability to perform key safety functions.

RISK MANAGEMENT VERIFICATION PHASE

The resident inspection staff is not expected to verify the validity or appropriateness of the licensee's risk categories or bands or the risk reduction effectiveness of prescribed RMAs. That is reserved for supplemental inspection if necessary. For the purposes of this IP, the inspectors are only expected to verify that licensee-established risk categories are recognized and entered according to an adequate RA and that the associated normal work controls or RMAs are effectively implemented in accordance with licensee procedures.

Block 15 - Were Normal Work Controls Authorized? (11.3.7)

Determine if normal work controls are authorized (low-risk configurations) or if RMAs were required by licensee procedures, the RA results and associated licensee risk category. Industry guidance prescribes instituting RMAs if ICDP will exceed 1.0×10^{-6}, but this is not a regulatory requirement, and as stated above, individual licensee risk categories may deviate from the guidance. If normal work controls are authorized by licensee procedures for the effective risk level (assuming an adequate RA), no additional actions to manage risk (i.e., RMAs) are necessary for the configuration being considered. If normal work controls

were authorized, proceed to Block 17. If RMAs were required, proceed to Block 16. Use information from Block 12 to help answer this question.

Block 16 - Risk Management Actions (11.3.7.3)

In accordance with licensee procedures RMAs should be implemented in a graduated manner, commensurate with various increases above the plant's baseline risk. However, the risk reduction benefits of these actions are generally not quantifiable. These actions are aimed at increasing the risk awareness of key plant personnel, providing more rigorous planning and control of maintenance activities, and controlling the duration and magnitude of the increased risk. RMAs should be considered in the development of work schedules in accordance with the licensee's program and procedures. RMAs can include (but are not limited to) the following:

1. Actions to provide increased risk awareness and control

   - Discussion of planned maintenance activity with the affected operating shift(s). Ensuring operator awareness of risk level, RMAs, protected SSCs, contingency plans, etc., and obtain operations approval. Documenting risk information in logs, on status boards, etc
   - Conducting pre-job briefing of maintenance personnel, emphasizing risk aspects of planned maintenance evolution
   - Requesting system engineers to be present for the maintenance activity, or for applicable portions of the activity
   - Obtaining plant management approval of the proposed activity
   - Ensuring risk and RMA information on all work schedules, plans, etc.
   - Announcing the plant risk band in effect and what risk-significant activities are in progress on the public system (e.g., Gaitronics) periodically and when changes occur.

2. Actions to reduce duration of maintenance activity

   - Pre-staging parts, materials, tools and other equipment
   - Walking down tagouts, equipment lineups (e.g., valves and switches) and the maintenance activity prior to starting work
   - Conducting training on mockups to familiarize maintenance personnel with the activity (similar to ALARA strategies)
   - Working jobs during back shifts as well as day shift
   - Establishing contingency plan to restore out-of-service equipment (or functions) rapidly if needed

3. Actions to minimize magnitude of risk increase

   - Minimizing other work in areas that could affect initiators (e.g., reactor protection system areas, switchyard, emergency diesel generator rooms, switchgear rooms) to decrease the frequency of initiating events that are mitigated by the function performed/supported by the out-of-service SSC

- Minimizing other work in areas that could affect other redundant systems (e.g., high pressure coolant injection/reactor core isolation cooling rooms, auxiliary feedwater pump rooms)

- Establishing alternate success paths for performance of the safety function of the out-of-service SSC (note: equipment used to establish these alternate success paths need not be within the scope of the maintenance rule). Use of administrative controls to ensure that backup equipment is protected.

- Establishing other compensatory measures

- Re-prioritizing and/or rescheduling maintenance activities

4. A final action threshold should be established so that risk significant configurations are not normally entered voluntarily.

Handling Temporary Alterations

Regulatory Treatment of Compensatory Measures

Compensatory measures (including temporary alterations or modifications) may be employed, either prior to or during maintenance activities, to facilitate the work as well as to mitigate risk impacts. The following guidance discusses the applicability of 10 CFR 50.65 (a)(4) and 10 CFR 50.59 to the establishment of temporary alterations or modifications. There are two circumstances of interest:

1. The temporary alteration serves as a compensatory measure, established to address a degraded or nonconforming condition, and will be in effect prior to conduct of maintenance to restore the SSC's condition. Per NRC Generic Letter 91-18, Revision 1, and NEI 96-07, Revision 1, the compensatory measure should be reviewed under 10 CFR 50.59. Since the compensatory measure is in effect prior to performance of the maintenance activity, no RA is required under 10 CFR 50.65 (a)(4).

2. The temporary alteration is related only to the maintenance activity and is established to facilitate the work and/or as a risk management action to reduce risk during a maintenance activity. The 10 CFR 50.65 (a)(4) RA should be performed to support the conduct of the corrective maintenance and address those temporary alterations or compensatory measures that will be in effect during performance of the maintenance activity. The compensatory measures would be expected to reduce the overall risk of the maintenance activity; however, the impact of the measures on plant safety functions should be considered as part of the (a)(4) RA. Since the compensatory measures are associated with maintenance activities, no review is required under 10 CFR 50.59 unless the measures are expected to be in effect during power operation for greater than 90 days. See NEI 96-07, Revision 1, dated November 2000, Reg Guide 1.187, and NRC Inspection Manual Part 9900 for guidance.

If RMAs were initiated in accordance with licensee procedures, proceed to Block 17. If not, proceed to Block 9.

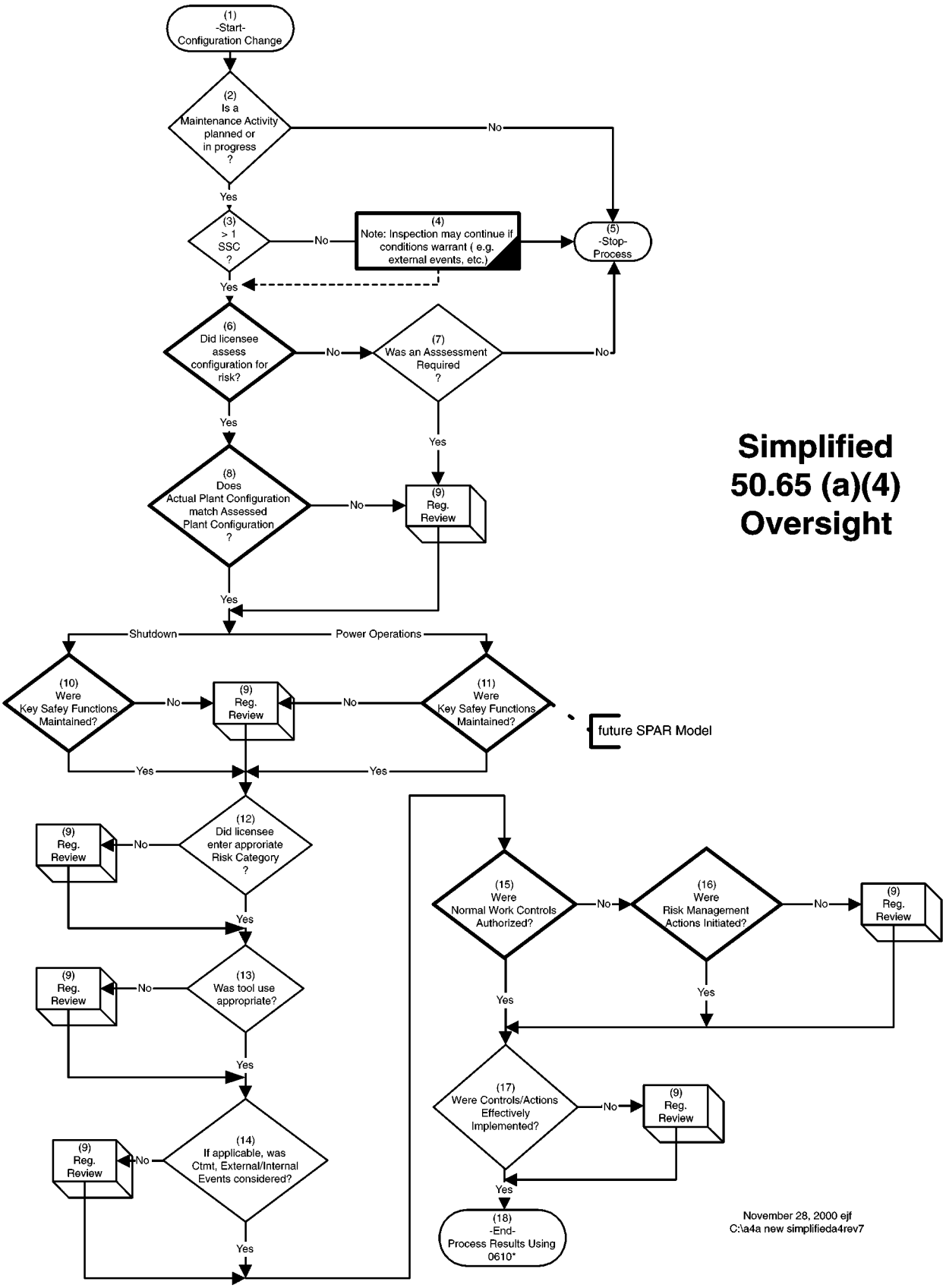
Block 17 - Was the Method of Managing Risk Effectively Implemented? (11.3.8)

Using licensee procedures, verify that the licensee effectively implemented the RMAs or normal work controls prescribed for the existing licensee risk category or band and consistent with the RA results. RMAs can be verified in conjunction with routine plant tours

or walkdowns in addition to reviewing documentation, attending briefings, examining equipment, and interviewing licensee personnel. For example, if one train of an important system is out of service, verify that the other train is fully available. Also, the inspector should review the manner in which the licensee handled temporary alterations or modifications associated with maintenance. If the licensee entered the appropriate licensee risk category, effectively implemented the prescribed RMAs or normal work controls, and appropriately controlled the temporary alterations, proceed to Block 18. If not, proceed to Block 9.

Block 18 - End Process

Perform a final evaluation and screen the issues that arise in the course of this inspection (from Block 9) in accordance with Appendix B of MC 0612. If indicated, determine the significance of the findings using the Reactor Safety SDP. Document the findings in accordance with MC 0612.


(1) -Start- Configuration Change
(2) Is a Maintenance Activity planned or in progress ?
No
Yes
(3) > 1 SSC ?
No
(4) Note: Inspection may continue if conditions warrant (e.g. external events, etc.)
(5) -Stop- Process
Yes
(6) Did licensee assess configuration for risk?
No
(7) Was an Asssessment Required ?
No
Yes
Yes
(8) Does Actual Plant Configuration match Assessed Plant Configuration ?
No
(9) Reg. Review
Yes
Shutdown
Power Operations
(10) Were Key Safey Functions Maintained?
No
(9) Reg. Review
No
(11) Were Key Safey Functions Maintained?
future SPAR Model
Yes
Yes
(9) Reg. Review
No
(12) Did licensee enter approriate Risk Category ?
Yes
(9) Reg. Review
No
(13) Was tool use appropriate?
Yes
(9) Reg. Review
No
(14) If applicable, was Ctmt, External/Internal Events considered?
Yes
(15) Were Normal Work Controls Authorized?
No
(16) Were Risk Management Actions Initiated?
No
(9) Reg. Review
Yes
Yes
(17) Were Controls/Actions Effectively Implemented?
No
(9) Reg. Review
Yes
(18) -End- Process Results Using 0610*
Simplified 50.65 (a)(4) Oversight
November 28, 2000 ejf
C:\a4a new simplifieda4rev7