IMPLEMENTING THE GRADED APPROACH PROCESS AT THE DEPARTMENT OF ENERGY FACILITIES

TO

PAAA WORKING GROUP

Submitted by The Graded Approach Task Team:

Lynne Adams, Sandia
Adam Cohen, Argonne National Lab
Roy H. Lebel, Brookhaven National Lab
Robert W. Swatek, Shaw Environmental, Inc.– NTS
Brinley D. Varchol, Fluor Fernald
Mike Walls, ORNL
Steve Ward, Sandia

David Ponke, Writer/Editor
Fluor Fernald

Revision 1
10/01/2002

ACKNOWLEDGEMENTS TO: **Jay N. Davis, BBW1-INEEL**

Al Elliot, LANC

Abel Garcia, LLNL

Chuck Mosley, Y-12

GRADED APPROACH

This document was designed to help Price Anderson Amendments Act (PAAA) Coordinators be consistent in the application of the graded approach at DOE facilities. The goal is to establish a common understanding and facilitation of the graded approach process and to provide a written reference to reduce ambiguity. At the same time it is recognized that every situation is unique and that you must adapt the graded approach that best fits your circumstances.

The information within, while detailed and thorough, is for informational purposes and is not meant to replace the official descriptions or orders controlled by the DOE.

RECORD OF ISSUE/REVISIONS

EFFECTIVE DATE	REV. No.	DESCRIPTION
04/01/2002	0	Issue for EFCOG Working Group Review
10/01/2002	1	Incorporations of appropriate comments from EFCOG Working Groups

TABLE OF CONTENTS

ATTACHMENTS

Note: The Attachments listed are examples of processes currently used at one or more DOE facilities and are provided for information or reference purposes.

INTRODUCTION

1.0 Purpose

The purpose of this document is to provide a tool for Price Anderson Amendments Act (PAAA) Coordinators to support a Graded Approach process at their facility. It provides examples, background information, and established process that should prove useful to PAAA Coordinators.

The document addresses a process consistent with 10 CFR 830, *Nuclear Safety Management*. 10 CFR 830 governs the conduct of DOE contractors, DOE personnel, and other persons conducting activities (including providing items and services) that affect, or may affect, the safety of DOE Nuclear Facilities.

2.0 SCOPE

The Graded Approach must be implemented without compromising the safety of the public, employees or facilities; adversely impacting the environment; or failing to comply with U.S. Department of Energy (DOE) requirements, rules, and regulations. The graded application of facility/activity requirements is dependent on the level of risk associated with the activity under consideration. Per 10 CFR 830.7, "Where appropriate, a contractor must use a graded approach to implement the requirements of this part, document the basis of the graded approach used, and submit that documentation to DOE."

DOE Nuclear Facilities

- Contractors conducting activities, including providing items or services, that affect, or may affect, the nuclear safety of DOE nuclear facilities must conduct work in accordance with the Quality Assurance Criteria in Subpart A--Quality Assurance Requirements of 10 CFR 830. This Subpart applies to activities that have the potential to cause radiological harm.

- A contractor must perform work in accordance with the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility and, in particular, with the hazard controls that ensure adequate protection of workers, the public, and the environment in accordance with Subpart B--Safety Basis Requirements of 10 CFR 830.

3.0 Fundamental Premise of the Graded Approach Process

The Graded Approach Process is based on the fundamental premise that Facility/Activity requirements must be applied in a manner consistent with:

- Hazards & Complexity of the work including:
  - safety, safeguards, & security
  - radiological & non-radiological hazards

- Relative risk to:

- workers, environment, public
- facility
- programmatic mission
- corporation and the client

Graded Approach means the process of ensuring that the level of analysis, documentation, and actions used to comply with a requirement in this part are commensurate with:

(1) The relative importance to safety, safeguards, and security (Level of Risk);
(2) The magnitude of any hazard involved;
(3) The lifecycle stage of a facility (Age, status, and condition of Facility or Process);
(4) The programmatic mission of a facility (Complexity of products or service involved);
(5) The particular characteristics of a facility;
(6) The relative importance of radiological and nonradiological hazards; and
(7) Any other relevant factors.

Above all, however, it must be remembered that the Graded Approach Process cannot be used to "**grade to zero**" (i.e., eliminate requirements). Even in the least stringent application of the Graded Approach Process, compliance with applicable portions of stated requirements is mandatory. An "exemption" process can be used to eliminate requirements but that process is separate and distinct from the graded approach.

4.0 Integrated Safety Management (ISM)

During the implementation of work, workers must incorporate the seven guiding principles and five core functions of Integrated Safety Management (ISM). ISM requires both DOE and Contractor to systematically integrate safety into management and work practices at all levels so that the mission is accomplished while protecting the public, the worker, and the environment. This is to be conducted through effective integration of Integrated Safety Management into all facets of work planning and execution. ISM is also consistent with the safety basis requirements of hazard category 1, 2, or 3 DOE nuclear facilities.

5.0 Document Organization

This document is divided into six (6) sections, the first four, which describes a step in the Graded Approach Process and the last two, a Definition list and a Bibliography that lists all sources and references utilized in the development of this document. Also included is a Graded Approach Process Flowchart. Each section provides a description of the associated step, as well as examples of how the associated action(s) could be performed. Given the nature of this document, the "process examples" are intended to serve as a starting point for documenting a site Graded Approach Process, and are in no way intended to represent the only correct manner in which to arrive at the end result.

The four sections are:

I PRELIMINARY ANALYSIS

II IDENTIFICATION OF APPROPRIATE REQUIREMENTS

III PRELIMINARY ANALYSIS OF ASSOCIATED RISK

IV COMMUNICATION AND IMPLEMENTATION

SECTION I
PRELIMINARY ANALYSIS

1.0 Purpose

This section will provide an overview description of the basic process for performing a Facility/Activity preliminary analysis to aid in ensuring the application of appropriate controls are put in place commensurate with risk.

Hazards taken into account during this analysis should include, but are not limited to, potential impact to the worker, public health and safety, and threats to the environment, as well as programmatic issues such as business impacts resulting from loss of operability, regulatory enforcements, and loss of customer confidence.

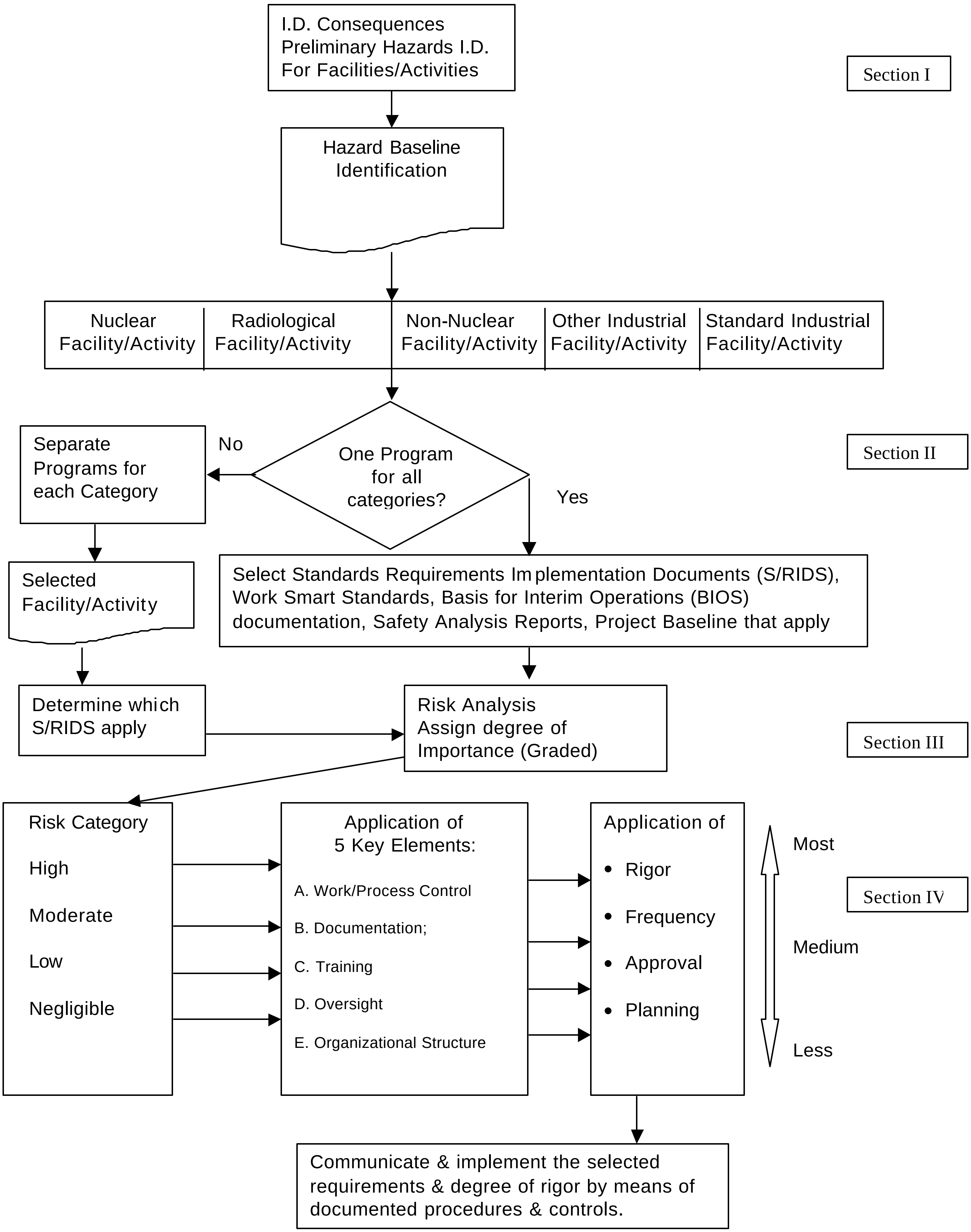
Once completed, the preliminary analysis will form the basis for the overall Graded Approach process for the Facility/Activity, and will be used in the work planning process during the development and design stages of and procurement for a project, program, experiment, study, process, or system. It may also be used during the development of new procedures where a graded approach to Quality is applicable.

2.0 Process Description

The activity or facility hazard category determines the level of hazard baseline documentation required by DOE per DOE-STD-1027-92, Change Notice #1. The hazard categorization of facilities is a multi-step process that results in a facility being categorized as Nuclear, Radiological (RadF), Non-nuclear, or Other Industrial Facility (OIF). The hazard categorization of Nuclear Facilities is accomplished by in-depth safety analysis documented in approved Basis for Interim Operations (BIOs), Safety Analysis Reports (SARs), Documented Safety Analyses (DSAs) for the types of facilities identified in Table 2 of 10 CFR 830 Subpart B, Appendix A, column 1. Column 2 of the same table has the “Safe Harbor” provision that shows the appropriate DOE requirements documents to be used in developing the DSAs. Facilities other than nuclear facilities are categorized and documented in an approved document or an approved Safety Assessments (SAs) and/or Auditable Safety Analysis.

The methodology used for conducting the hazard categorization must be consistent with DOE-STD-1027-92, Change Notice #1. Other standards recognized by DOE may be used to augment their analysis. In principle, the releasable inventory of hazardous materials within a facility are compared to Threshold Quantities (TQs) established by the guidance documents. Therefore facilities can be "bundled" according to their potential hazards and hazard baseline documentation requirements can then be assigned to the facilities using a graded approach.

GRADED APPROACH PROCESS FLOWCHART



3.0 Process Example to Perform Preliminary Analysis

Using the process outlined in DOE-STD-1027-92, Change Notice #1 (or another hazard identification process as detailed in site-specific guidance) perform and document the Facility/Activity Hazard Baseline, and categorizes facilities/activities as one of the following:

- Nuclear Facility/Activity,
- Radiological Facility/Activity,
- Non-Nuclear Facility/Activity,
- Other Industrial Facility/Activity, or a
- Standard Industrial Facility/Activity.

Hazard Category

A site, Hazard Survey and Hazard Assessment document, presents and updates the results of the facility-specific hazard assessment to provide a technical basis for facility emergency planning efforts and to provide a preliminary hazard categorization for site facilities based on an inventory of hazardous materials. A final Hazard Category can be based on an assessment of the consequences resulting from postulated bounding accident scenarios.

Assessment Criteria - Hazard Assessment can be conducted in accordance with the following:

- DOE Order 151.1, Comprehensive Emergency Management System;
- DOE-STD-1027-92, Change Notice #1, Hazard Categorization and Accident Analysis Techniques for compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports; or
- another hazard assessment identification process recognized by DOE as detailed in site-specific requirements.

Scope

Categorization and Classification of Buildings - Within a site document, categorization refers to the cataloging of buildings via safety analysis documentation while classification refers to Emergency Preparedness Classes.

Categorization Of Buildings - Nonreactor Nuclear Facilities are categorized in site document, the DOE-approved Basis for Interim Operations (BIOs) or Safety Analysis Reports (SARs). Non-nuclear Facilities and operational Radiological Facilities (RadF) are documented in a separate Auditable Safety Analysis. The remaining site facilities are categorized either by separate safety analysis or a stand-alone hazard assessment.

The analytical basis for the nuclear facility/building category may be contained in a site Implementation Plan for SARs and TSRs at the DOE sites. Buildings that are not Nuclear (i.e., RadF, Non-nuclear, and Other Industrial Facilities (0IF)) are preliminarily categorized based on their releasable hazardous materials inventories.

Hazard Categorization - A site Hazard Survey and Hazard Assessment document serves the following distinct purpose, Hazard Categorization of buildings/activities for determining safety analysis documentation and associated controls.

Hazard Categorization Methodology - The building hazard category determines the level of hazard baseline documentation required. The hazard categorization of facilities is a multi-step process that results in a facility being categorized as Nuclear, Radiological (RadF), Non-nuclear, or Other Industrial Facility (OIF). The hazard categorization of Nuclear Facilities is accomplished by in-depth safety analysis documented in a site document, BlOs, or DOE approved Safety Analysis Reports SARs). Facilities other than nuclear facilities are categorized and documented in this report or Safety Assessments (SAs) and/or Auditable Safety Records (ASRs) that are available from Safety Analysis.

Standard Methodology - The methodology used for conducting the hazard categorization is consistent with DOE-STD-1027-92, Change Notice #1. In principle, the releasable inventory of hazardous materials within a facility are compared to Threshold Quantities (TQs) established by the guidance documents. Therefore facilities can be "bundled" according to their potential hazards and hazard baseline documentation requirements can then be assigned to the facilities using a graded approach.

4.0 Use of Single or Multiple Graded Approach Programs

Attachment 2, “Determination of Single or Multiple Graded Approach Programs,” describes the decision-making process used to determine whether a single all-encompassing Program have been implemented, or whether individualized Programs for each Nuclear Safety Management program are utilized.

Prior to advancing further in the development of the Graded Approach Process, Facility/Activity Management must determine whether one Graded Approach Program, which encompasses all Hazard Categories, will be developed, or whether individualized Graded Approach Programs for each Hazard Category would be more appropriate. Regardless of this determination, the next step in the process is to identify Standards.

SECTION II

IDENTIFICATION OF APPROPRIATE REQUIREMENTS

1.0 Purpose

The purpose of this section is to describe a process used to identify requirements that are applicable to the Facility/Activity. Examples of these requirements include:

- Standards Requirements Implementation Documents (S/RIDS)
- Work Smart Standards (WSSs)
- Basis for Interim Operations (BIOS) documentation
- Safety Analysis Reports (SARs)
- documented Safety Analysis (DSAs)
- Project Baseline

Other documentation as deemed appropriate and/or directed by Facility/Activity Management and the site contractor.

2.0 Process Description

This section should describe the process a site uses to evaluate requirements from their contract and codes, standards and regulations to ensure their incorporation into site requirements. For example:

A. Approach

Site has identified and reviewed the requirements that are applicable to the Facility/Activity based on the contract requirements. The review should be done in consort with the customer and ensure that the contract requirements are adequate for the desired hazard and management controls.

B. Description

Each major project may develop a Project Execution Plan or similar document that outlines the requirements implemented in their project. Work activities are conducted through a work authorization process utilizing the principles of integrated safety management. The requirements for business performing and conducting work are outlined in the prime contract and documented in requirement manuals that establishes a single program for each functional area.

SECTION III

ANALYSIS OF ASSOCIATED RISK

1.0 Purpose

This section describes a process that may be used by the site to analyze risk and document the results. Facility/Activity Management may assign a quantitative level of implementation for the identified requirements based on: 1) the consequences associated with a failure to adhere to identified requirements and 2) the probability that a failure to adhere to the identified requirements would occur.

2.0 Process Description

Section I analysis should be used as a starting point for this analysis. There are many processes, which can accomplish this task. Section 1 describes the first step in the performance and documentation of an Analysis of Associated Hazard for the Facility/Activity. After Hazard Categorization is determined, then performance grading and risk evaluation for structures, systems and components (SSCs) may be performed. This performance grading and risk evaluation ensures that the level of detail required for analysis, documentation, application of engineering principles, and operations that comply with requirements is commensurate with relative importance to safety (Hazard Category), programmatic risk, complexity of the activity, facility life cycle, or importance to a site mission.

3.0 Process "Example" to Perform and Document an Analysis of Associated Risk

Based on the consequences associated with a failure to adhere to identified requirements and the probability that a failure to adhere to the identified requirements would occur, Facility/Activity Management may assign a quantitative level (i.e., Risk Category or Quality Classification) of implementation for the identified requirements.

A. Approach

Section 1 describes the performance and documentation of an Analysis of Associated Hazards for the Facility/Activity.

In order to accomplish this in a logical and consistent manner the development of a table that outlines the risks as well as levels or Quality classification (See Attachment 1, Table 1 "Screening Guidelines for Work Planning & Control and the Application of the Quality Graded Approach") may be used. In the development of the table relevant risk to your particular facility/function should be considered.

Using the criteria in Table 1, consider the following when reviewing for the application of a graded approach:

- The graded approach (e.g., Quality Classification) should be based on the programmatic and/or ES&H impact.

- The classification assigned to a subsystem or process may be more significant than the classification assigned to the overall system, process or experiment (i.e., System = A-3 and Subsystem = A-2). Similarly, the classification assigned to the lower levels may be more significant than the preceding level, (i.e., Assembly = A-3 and Subassembly = A-2).

- Although an attempt has been made to quantify the adverse impacts, judgment and adequate margins of safety must be considered when selecting a classification.

Costs should include all expenses, e.g., replacement cost, cost of labor, downtime, cleaning (including decontamination), renovating, replacing, or rehabilitating structures, equipment, or property.

After considering all appropriate issues/risks, select the appropriate Risk Category or Quality classification that best describes where your Facility/Activity lies.

B. Description

B.1 Evaluation Basis Accident (EBA)

An EBA is a hypothetical accident postulated for evaluation of the performance of a facility for which documentable design basis accidents do not exist. The intent of the EBA is to derive from facility parameters an accident that can be used to determine the potential consequences of functional failures in mitigating or preventive systems.

Accident Analysis – Dominant credible accident scenarios that could result in significant impact are analyzed to a level of detail sufficient to identify areas where operational flaws could constitute vulnerabilities. The severity of the consequences for each postulated event should be based on a comparison to the consequences of the evaluation basis accidents (EBAs) for the facility. The EBAs are those events, which have the potential for the greatest impact on co-located workers, the public, or the environment. The intent of the EBA calculation is to probabilistically derive an accident that can be used to determine the potential consequences of functional failures in mitigative or preventive systems, and to compare those consequences to preset guidelines used for hazard classifications. The EBA analyses are very conservative because:

- All the facility dispersible inventory is at risk for earthquake and high wind event,

- The release values attributed to each ruptured container are conservative when compared to demonstrated values, (DOE Order 5480.23)

- No credit should be taken for building containment of released materials.

The following currently define nuclear Hazard Categories:

- **Category 1:** The hazard analysis shows the potential for significant off-site consequences.

- **Category 2:** The hazard analysis shows the potential for significant on-site consequences. The requirements are essentially a facility with a potential for nuclear criticality or the possession of quantities of material whose unmitigated release could produce total doses of 1 rem or greater in the range of 100 meters from the facility.

- **Category 3:** The hazard analysis shows the potential for significant but localized consequences. The requirement is essentially possession of quantities of material whose unmitigated release could produce effective whole body doses of less than 10 rem at 30 m from the source area.

Radiological Facilities

Radiological Facilities are those facilities that do not meet or exceed the hazard category 3 threshold quantity values published in DOE-STD-1027-92, Change Notice #1, Change Notice #1 but still contain some quantity of radioactive material (above those discussed in Appendix B to 40 CFR 302).

Hazard Class

Non-nuclear facilities may be classified as high, moderate, or low hazards based on the following:

- High – hazards with a potential for onsite impacts to large numbers of persons or for major impacts to the environment,

- Moderate – hazards which present considerable potential onsite impacts to people or the environment, but at most only minor offsite impacts, and

- Low – hazards, which present minor onsite and negligible offsite impacts to people and the environment.

Industrial Facility (IF)

- **Other Industrial Hazard (OIH)** – Other Industrial Hazard facilities are standard industrial hazard facilities, which have the potential for radiological or other form of contamination and may require a Radiation Work Permit (RWP) or other permit in order to perform the work. The hazards associated with OIH are fully addressed in established site programs, such as the Radiation Protection and do not need any unique treatment.

- **Standard Industrial Hazards (SIH)** – These are facilities whose hazards are routinely encountered in general industry and construction, and for which national consensus codes and/or standards (e.g., OSHA, transportation safety) exist to guide safe design and operation without the need for special analysis to define safe design and/or operational parameters (DOE-STD-3009-94, Change Notice #1)

B.2 Performance Grading (PG)

Purpose – Site Procedure for Performance Grading may establish and provide for performance grading and risk evaluation of structures, systems, and components (SSC). Performance grading ensures that the level of detail required for analysis, documentation, and application of engineering principles that comply with requirements is commensurate with relative importance to safety (Hazard Category/Class (HC/C)), programmatic risk, complexity of the activity, facility life cycle, or importance to the Site mission.

Scope – Site Procedure for Performance Grading may be applicable to projects and activities performed or managed by the contractor where the level of detail is specified for analysis, documentation, and application of requirements and resources. The grading criteria and procedure describing Performance Grading should be used by the project organizations in establishing the level of control when accomplishing activities which are identified under Functional Areas (FA) such as Configuration Management (CM), Engineering Design (ED), Construction (CT), Operations (OP), Maintenance (MT), Nuclear and System Safety (NS), Packing & Transportation (PT), and Quality Assurance (QA). "Note: Grading for these functions must be accomplished in accordance with allowed functional requirements." These functional areas include the design organizations of site Facility/Technical Engineering, Architect-Engineers, and service subcontractors implementing performance specifications.

A performance Grade (PG) should be assigned to each SSC based on the steps outlined in the site procedure for performance grading. These criteria originate from DOE Standard 1073-93, Parts one and two.

Performance Grade (PG) - Performance Grade is the numerical value assigned to classify a System, Structure, or Component as it relates to an activity or function. The engineer assigns a performance grade (PG) to an activity or SSC in terms of five criteria. These criteria are:

- Safety considerations involving the consequences of its failure to prevent or mitigate the release of radioactive materials or energy, or hazardous materials.

- Mission importance considerations involving the consequences of its failure impacting schedule delay, stakeholder reaction, or project cost.

- Life-Cycle Considerations involving the design life or intended use/consequence of the SSC or Project.

- Complexity considerations involving the degree of regulatory, design, construction, process, and/or management coordination required.

- Risk considerations based on the grading risk evaluation.

Structures, Systems and Components (SSC) – For classic engineering, procurement, construction projects, typical SSCs are as follows: Structures are elements that provide support or enclosure such as buildings, free standing tanks, basins, dikes, and stacks. Systems are collections of components assembled to perform a function such as piping, cable trays, conduit, or HVAC. Components are items of equipment such as pumps, valves, relays, or elements or a larger array such as computer software, lengths of pipe, elbows, or reducers.

For other projects to accomplish site remediation such as D&D, Soils Excavation, Water Treatment, typical SSCs are as follows: Structures are elements that provide support or enclosure such as temporary buildings, basins, dikes, and supports. Systems are collections of components assembled to perform a function such as HEPA systems, water collection/diversion systems, water treatment, and monitoring systems. Components are items of equipment such as sediment barriers, liners, level controls, special monitors, and flow measurement.

The following “Definition Matrix “ is shown as an example of how grading can be established.

Performance Grade (PG) Definition Matrix

PG-1 - A SSC must be assigned a Performance Grade 1 (PG-1) if it is part of a "safety" system in a Hazard Category 1 (HC-1) or a High Hazard (HH) classification facility. Also whose breakdown (failure) fails a preventative or mitigative function necessary to insure that there is no unacceptable off-site risk.

PG-2 - A SSC must be assigned a Performance Grade 2 (PG-2) if it is part of a "safety" system in a Hazard Category 2 (HC-2) or a Moderate Hazard (MH) classification facility. Also, whose breakdown (failure) fails a preventative or mitigative function necessary to insure that there is no unacceptable on-site risk.

PG-3 - A SSC must be assigned a PG-3 if it is not covered under PG-1 or PG-2, and if any of the following conditions apply:

- The SSC is part of a "safety" system in a HC-3 or Low Hazard (LH) classification facility. Also, whose breakdown (failure) fails a preventative or mitigative function necessary to insure that there is no unacceptable risk to project workers, and;
- The SSC breakdown (failure) by itself or in combination with one or more SSCs may result in loss of function of emergency handling, hazard recovery, emergency preparedness, or emergency power system that may be needed to preserve the health and safety of the facility workers, collocated workers, and visitors.

PG-4 - A SSC that is not covered under PG-1, PG-2, or PG-3 must be placed in PG-4 if any of the following conditions apply:

- The SSC breakdown (failure) may cause a life threatening situation to activity workers or collocated workers, or
- A SSC is required to prevent or mitigate a Standard Industrial Hazard (SIH), or
- A SSC is part of a monitoring system that monitors compliance with regulatory imposed release limits.

PG-5 - A SSC that is not covered under PG-1 through 4 may be placed in PG-5 if is not important because of safety, mission, or cost considerations, except that a SSC whose breakdown (failure) may have an adverse effect on the performance of a PG-1, PG-2, PG-3, or PG-4 or SSC must not be placed in PG-5.

B.3 Mission Importance or Programmatic Risk

Attachment 3, "MISSION IMPORTANT CONSIDERATIONS AND SIMPLIFIED RISK ASSESSMENT", provides guidance for evaluating the mission importance or programmatic risk associated with a structure, system or component (SSC). The project engineer may identify relevant criteria for upgrading any SSC graded lower than a performance grade (PG) - 3 to a PG-3. A recommendation to upgrade the SSC must be prepared by the engineer for review and concurrence by the Technical Review Board (TRB).

NOTE: Mission Important criteria are those that the engineer would use to evaluate any PG-4 or PG-5 SSCs to see if there is justification to recommend that the SSC be upgraded to a PG-3 and may then come under Configuration Management.

This is an evaluation of all Stakeholder concerns, and the mitigating factors/programs that impact them. This final consideration is the foundation of a technical review, as it is the method by which a technical review board assures themselves that a management override of the safety derived PG's is or is not warranted. Mitigating factors are such things as use of controlled procedures, standard practices, engineering or administrative controls, etc. Each identified Stakeholder concern should be addressed separately and completely, with the documented positions presented to a technical review board.

B.4 Results of the Analysis Process

Attachment 4, "Facility Technical Basis and Authorization Table", is an example of the results of a documented analysis process that may be used at an Accelerator facility..

SECTION IV

COMMUNICATION AND IMPLEMENTATION

1.0 Purpose

The purpose of this section is to provide a description of how the overall Graded Approach Program requirements for a nuclear safety management process should be communicated to workers and the manner in which the requirements must be implemented.

A nuclear safety management program is designed to ensure a facility/activity is operated in a manner that adequately protects workers, the public, and the environment.

2.0 Process Description

Implementation of Facility/Activity requirements utilizing the Graded Approach philosophy may be achieved through the inclusion of a number of factors during the planning and execution phases. While individual sites should tailor the manner in which the Graded Approach process is implemented, generally speaking the methods of achieving this implementation fall into five (5) areas:

Work/Process Controls --	• Rigor of planning required for the Facility/Activity • Startup/re-start authorization
Documentation -------------	• Level of review, approval, detail and control
Training ----------------------	• Level of training required (Awareness/ Qualification/Certification)
Oversight ---------–------	• Frequency of oversight Independence of reviews, and Confidence level
Organizational Structure--	• Complexity of organizational structures • Appropriate levels of management and supervision • Reporting relationship and integration to the support functions

A. Work/Process Controls

A primary phase of Graded Approach implementation is the development of Work/Process Controls. This process identifies the steps taken by a Facility/Activity to manage both the intrinsic and extrinsic risks associated with a particular process through the implementation of administrative and/or engineered controls. These controls may consist of:

- Strict guidelines prescribing the rigor of planning required for the Facility/Activity

- Startup/re-start authorization guidelines (Operational Readiness Review/ Readiness Assessment/Standard Startup Review/Management Assessment)
- Clearly defined lines of authority for Authorization/Approval to Proceed
- Procedural requirements which provides both parameters for safe/efficient operations and operational limits (QA hold points, etc.) to ensure that work is performed and results achieved as planned

B. <u>Documentation</u>

Upon identification of the controls necessary for implementation of the Graded Approach process, these controls must be documented and communicated to Facility/Activity personnel. This documentation may take the form of written procedures, practices, requirements manuals, policy statements, Standing Orders, or other written and controlled means as deemed appropriate by Facility/Activity Management. The level of approval of this documentation is also based on the hazards, complexity, and relative risk.

C. <u>Training/Communication of Requirements</u>

Facility/Activity Management must identify and establish the means through which affected personnel are provided with an understanding of specific programmatic requirements. Depending upon Facility/Activity Management discretion, this communication of requirements may take the form of something as simple as a required reading of applicable documents, or may be as complex as a formal training program culminating in personnel certification/qualification. Regardless of the means of communication, the process for informing affected personnel of programmatic requirements should be developed and implemented in a manner which takes the relative risk(s) of the process being described into account, and the results/completion of the communication must be documented (via required reading sign-off sheets (or electronic equivalent), training rosters, qualification records, etc.).

D. <u>Oversight</u>

Facility/Activity Management should perform regularly scheduled oversight reviews in order to ensure that the Graded Approach process is adequately and consistently implemented. In keeping with the basic tenants of the Graded Approach philosophy, the scope and frequency of these oversight activities should be commensurate with the relative risk(s) involved. Types of reviews may include self-assessments, management assessments or walkthroughs, inspections, surveillances, and audits.

E. <u>Organizational Structure</u>

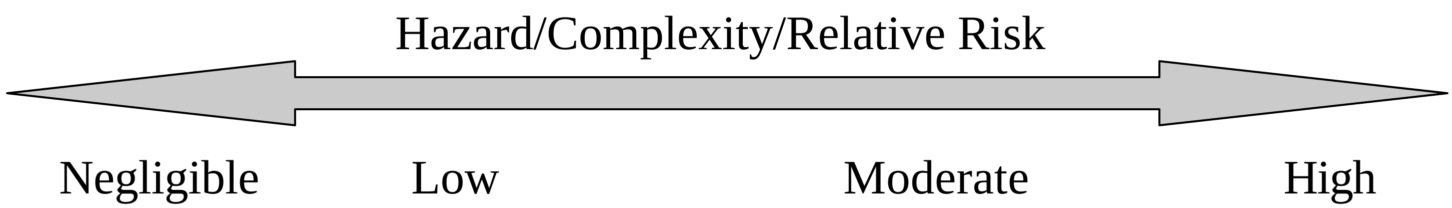
Facility/Activity Management should identify and establish the complexity of organizational structures, appropriate levels of management and supervision, and reporting relationship and integration to the support functions. The organizational structure may be based on the hazards, complexity, and relative risk of the work.

3.0 <u>Documents/Records Generated</u>

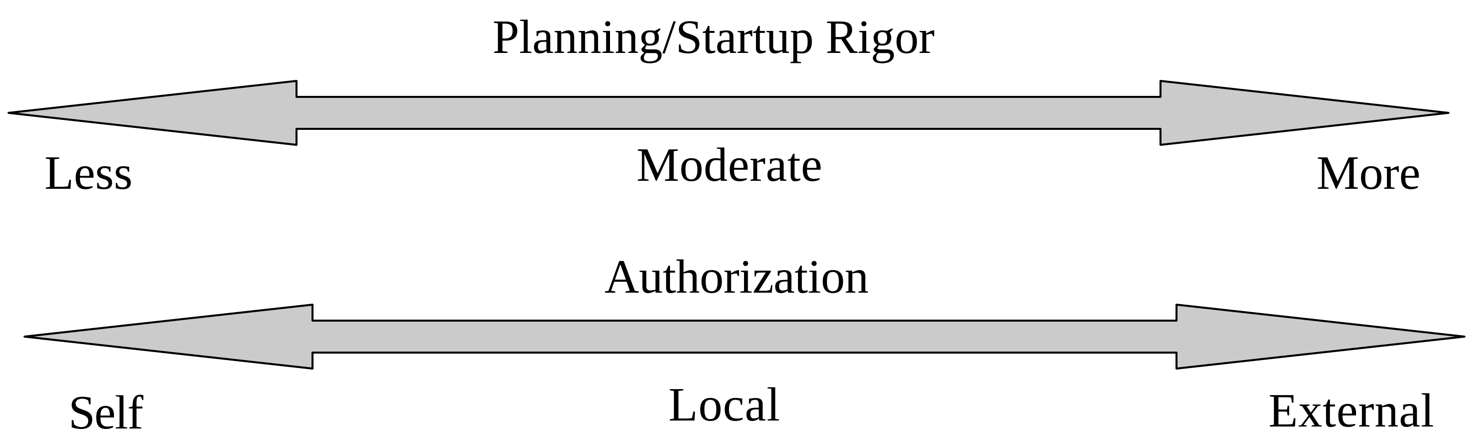
Documents and/or records generated by the process described in this section may include, but are not limited to, the following:

- Work planning documents (Project Execution Plans, Pre-operational Assessment Implementation Plans, Design Packages, Design Change Notices, etc.)
- Requirements documents (Procedures, Plans, Requirements Manuals, Practices, Standing Orders, etc.)
- Training materials (Lesson Plans, Briefing Plans, Training Rosters, Required Reading sign-off sheets, Personnel Qualification Records, etc.)
- Assessment/Oversight documentation and records (Surveillance Checklists and Reports, Inspection Reports, Audit Plans, Audit Checklists and Reports, Management Assessment Reports, Self Assessment Reports, Pre-Operational Assessment Reports, verifications, etc.)

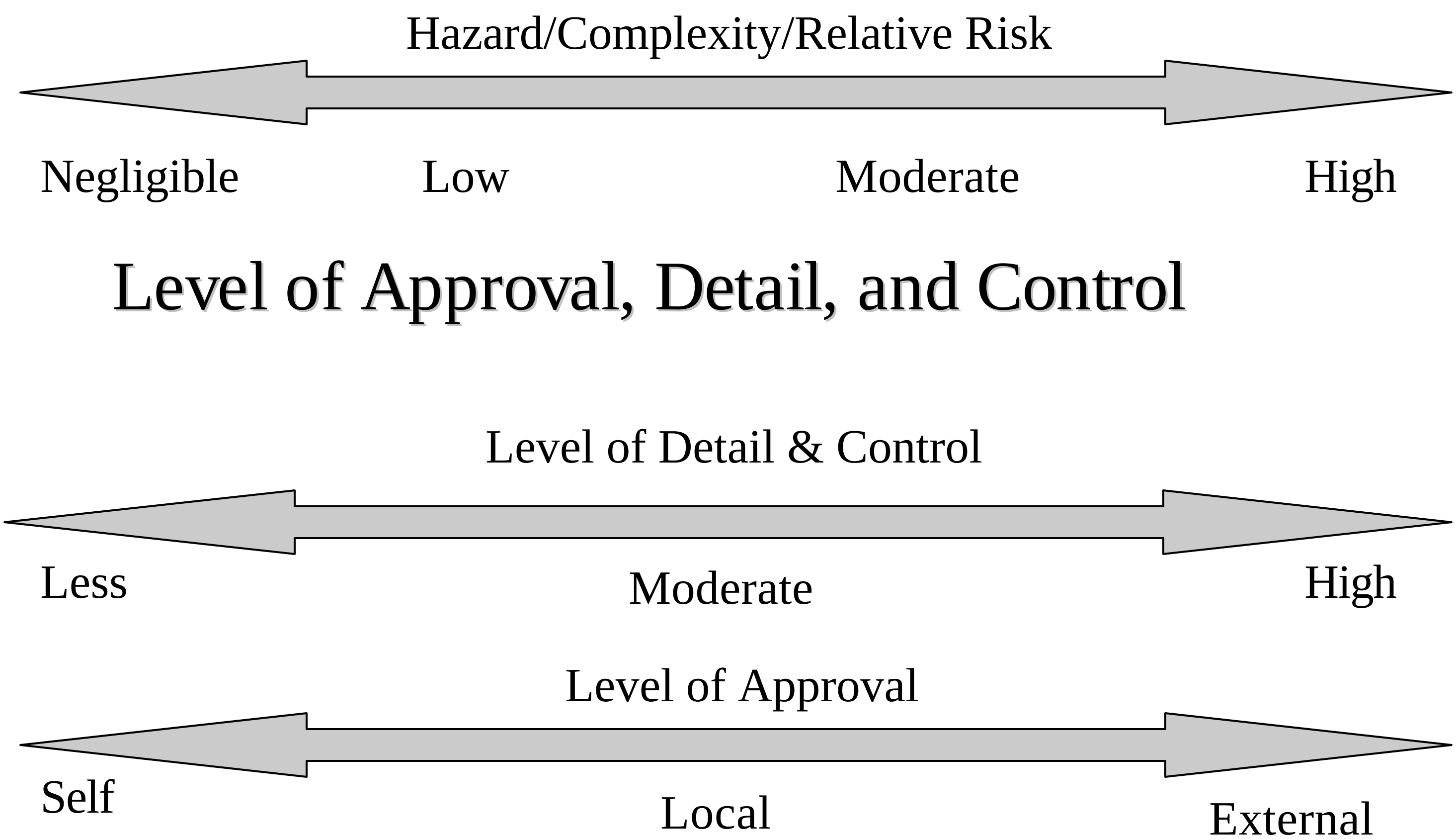
A. Work/Process Control



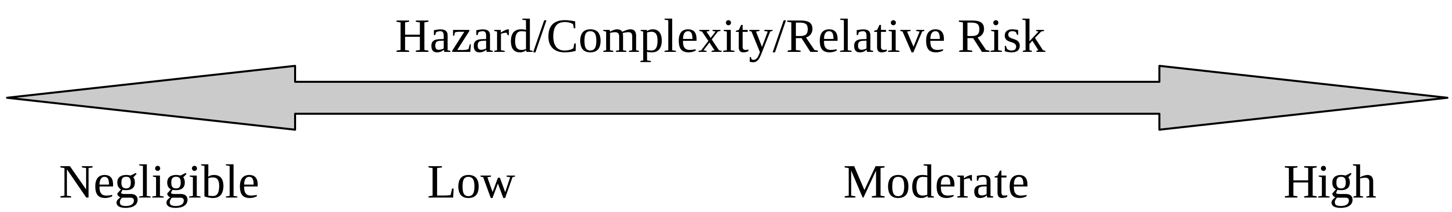
Rigor of Planning, Startup, and Authorization



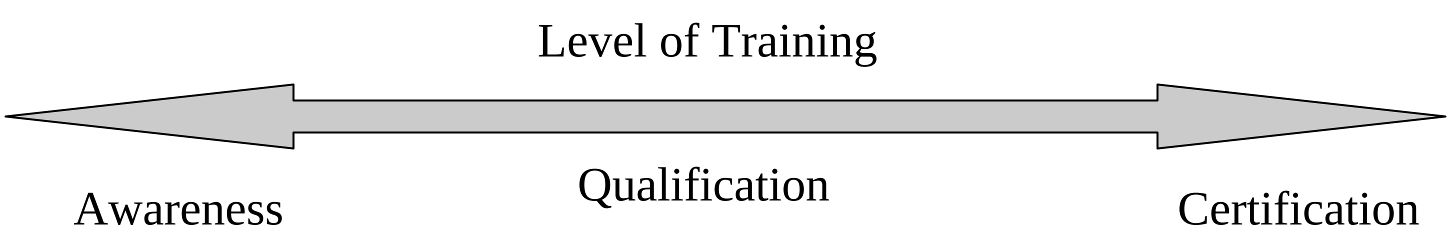
B. Documentation



C. Training



Awareness, Qualification, or Certification Process



D. Oversight

Hazard/Complexity/Relative Risk

Negligible — Low — Moderate — High

Frequency, Independence, and Confidence level

Frequency

Less (3 years) — Moderate (2 years) — Most (Annual)

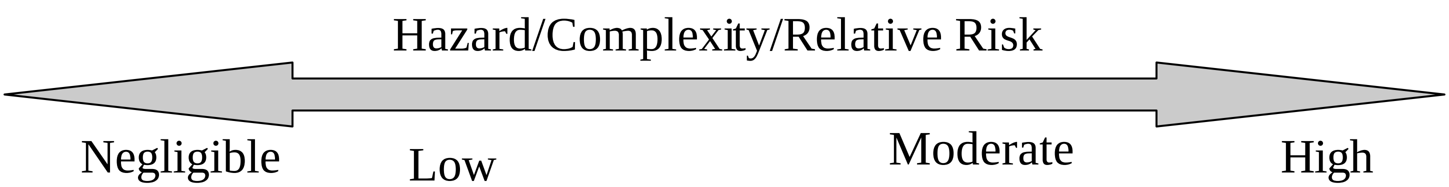
Breath & Depth

Less (Walk through) — Moderate (Surveillance/Inspection) — Most (Audit)

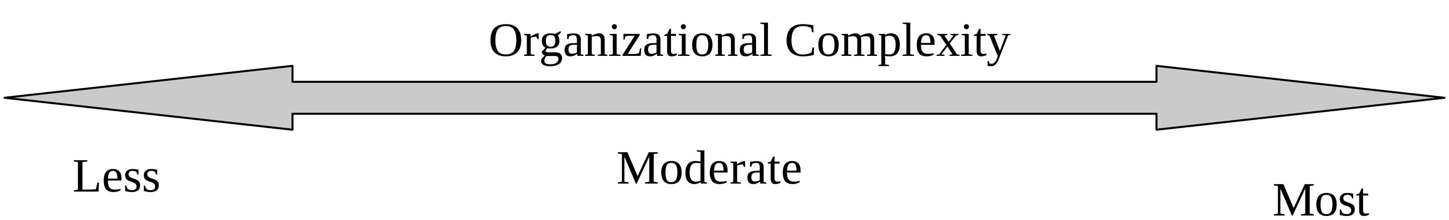
Independence

Self — Joint/Internal — Internal/External

E. Organizational Structure



Complexity of Reporting and Support Relationships



SECTION V

BIBLIOGRAPHY (INFORMATION/REFERENCE SOURCES)

10 CFR-820, Procedural Rules for DOE Nuclear Facilities

10 CFR Part 830, Nuclear Safety Management

40 CFR-302.4, Designation of Hazard Substances

DOE O 151.1, Comprehensive Emergency Management System

DOE N 203.1, Software Quality Assurance

DOE M 232.1-1A, Occurrence Reporting and Processing of Operations Information

DOE O 414.1A, Quality Assurance

DOE G 414.1-1, Implementation Guide for use with Independent and Management Assessment System Guide with 10 CFR 830.120 and DOE O 414.1

DOE G 414.1-2, Quality Assurance Management System Guide for use with 10 CFR 830.120 and DOE O 414.1

DOE O 430.1A: Life Cycle Asset Management

DOE O 5480.23, Nuclear Safety Analysis Reports

DOE-STD-1027-92 December 1992/Change Notice No. 1 September, 1997; Hazard Configuration and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports

DOE-STD-1073-93-Pt.1 November 1993, Guide for Operational Configuration Management Program

DOE-STD-3009-94, Change Notice #1, Preparation Guide for U.S. DOE Nonreactor Nuclear Facility Safety Analysis Reports

DOE-STD-3011-94, *Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23* (SAR) Implementation Plans

DOE-DP-STD-3023-98 April 1998, Guidelines for Risk-Based Prioritization of DOE Activities

DOE-EM-STD-5502-94 August 1994, Hazard Baseline Documentation

SECTION VI

DEFINITIONS

Activity - any program, project, or operation undertaken to plan, manage, integrate, or execute an environmental assessment, remedial design, remedial action, technology development, base function, or decontamination and decommissioning action.

Assembly - A number of subassemblies and/or components joined together to perform a specific function (i.e., pump, power supply, coil assembly, printed circuit board assembly).

Component - One piece or two or more pieces joined together which are not normally subject to disassembly without destruction of designed use (i.e., gear, screw, cam, transistor, resistor, integrated circuit, epoxy, adhesive.).

Facility - The buildings, utilities, structures, and other land improvements associated with an operation or service and dedicated to a common function. (DOE O 430.1A)

Graded Approach – The process of ensuring that the level of analysis, documentation, and actions used to comply with a requirement in this part are commensurate with: (10 CFR-830)

(1) The relative importance to safety, safeguards, and security;
(2) The magnitude of any hazard involved;
(3) The lifecycle stage of a facility
(4) The programmatic mission of a facility;
(5) The particular characteristics of a facility;
(6) The relative importance of radiological and nonradiological hazards; and
(7) Any other relevant factors.

Life-Cycle - The life of an asset from planning through acquisition, maintenance, operation, and disposition. (DOE O 413.1A)

Programmatic Risk - That risk associated with work at a site, which may upon failure cause schedule delays, cost overruns, or impact to stakeholders, such as the public, site workers, and regulating agencies.

Quality Classification - An indicator using a weighted scale that is used once the ES&H and programmatic risks have been evaluated, e.g., A1 (Critical), A2 (Major), A3 (Minor), and A4 (Negligible).

Risk - A concept used to give meaning to things, forces, or circumstances that pose harm or benefit to people, groups, or organizations, or to what they value. Descriptions of risk are typically stated in terms of the likelihood of harm or benefit from an activity and usually include an identification of what is "at risk" and may be harmed or benefited (e.g., health of human beings or an ecosystem, personal property, quality of life, ability to engage in an economic activity); the activity that may occasion this harm or benefit; and a judgment about the likelihood that harm or benefit must occur. (DOE-DP-STD-3023-98)

Subassembly - Two or more components combined into a unit for convenience in assembling or servicing. (i.e., beam tube with vacuum flanges, magnet trim coils).

Subsystem - A combination of assemblies, subassemblies, and components connected or associated together to perform an operational function (i.e., vacuum subsystem, cryogenic subsystem, magnet subsystem, tunnel).

System - A combination of subsystems, assemblies, subassemblies, and components joined together to form the finished product or prime level of assembly (i.e., accelerator, reactor, detector, building).

SSC Grade - A measure of the importance of structures, systems, and components (SSCs) within the facility, based on the most important design requirements applicable to the SSC, that can be used to determine priorities and proper levels of attention and resource allocations. An example of SSC grades and associated priorities is: (1) safety, (2) environmental, (3) mission, and (4) others. (DOE–STD–1073–93)

Structures, Systems, and Components (SSCs) -Structures are elements that provide support or enclosure such as buildings, free standing tanks, basins, dikes, and stacks. Systems are collections of components assembled to perform a function such as piping, cable trays, conduit, or HVAC. Components are items of equipment such as pumps, valves, relays, or elements of a larger array such as computer software, lengths of pipe, elbows, or reducers. (DOE–STD–1073–93)

ATTACHMENT 1, PAGE 1 OF 8

SCREENING GUIDELINES FOR WORK PLANNING & CONTROL AND APPLICATION OF THE QUALITY GRADED APPROACH

In order to accomplish this in a logical and consistent manner the development of a table that outlines the risks as well as levels or Quality classification (See Table 1 "Screening Guidelines for Work Planning & Control and the Application of the Quality Graded Approach") may be used. In the development of the table relevant risk to your particular facility/function should be considered.

Using the criteria in Table 1, consider the following when reviewing for the application of a graded approach:

- The graded approach (e.g., Quality Classification) should be based on the programmatic and/or ES&H impact.

- The classification assigned to a subsystem or process may be more significant than the classification assigned to the overall system, process or experiment (i.e., System = A-3 and Subsystem = A-2). Similarly, the classification assigned to the lower levels may be more significant than the preceding level, (i.e., Assembly = A-3 and Subassembly = A-2).

- Although an attempt has been made to quantify the adverse impacts, judgment and adequate margins of safety must be considered when selecting a classification.

Costs should include all expenses, e.g., replacement cost, cost of labor, downtime, cleaning (including decontamination), renovating, replacing, or rehabilitating structures, equipment, or property.

After considering all appropriate issues/risks, select the appropriate risk level or Quality classification that best describes where your Facility/Activity lies.

<u>High Risk</u> **-** Most stringent application of requirements
[Strict compliance + Additional work/process controls]

Note: Strict compliance may be assigned to sub elements of either High, Medium/Moderate, or Low Risk Facilities/Activities as necessary.

<u>Medium/Moderate Risk</u> **-** Less stringent application of requirements
[Compliance with applicable portions of stated requirements + Additional work/process controls]

<u>Low Risk</u> **-** Least stringent application of requirements
[Compliance with applicable portions of stated requirements]

ATTACHMENT 1, PAGE 2 OF 8

SCREENING GUIDELINES FOR WORK PLANNING & CONTROL AND APPLICATION OF THE QUALITY GRADED APPROACH

Extrinsic Risk – Risks associated with a process/activity which are the result of the performance of work associated with that particular process or activity, and which are above and beyond the inherent risks typically associated with that process or activity.

Intrinsic Risk – Risks associated with a process/activity, which are inherent to the operation or performance of that particular activity or process.

ATTACHMENT 1, PAGE 3 OF 8

Table 1
Screening Guidelines for Work Planning & Control and Application of the Quality Graded Approach

	ESH&Q Risk Level			
Risk Category	**Negligible**	**Low**	**Moderate**	**High**
Quality Class (Optional)	**A4-Negligible**	**A3-Minor**	**A2-Major**	**A1-Critical**
ES&H Issues				
1. Personnel Injury	Negligible risk for injury	Minimum risk for injury	Potential for serious injury	Potential for fatality or severe injury
2. Radiological Work	Negligible potential for exposure	Work in controlled areas	Work requiring an RWP	Work requiring an RWP and ALARA review
3. Electrical Work	De-energized (discharged) Work on any electrical system after proper application of LOTO and zero energy checks	• Work on energized systems 50 volts or less (Range A)	Work on energized systems greater than 50 volts but less than 600 volts	• Work on energized systems 600 volts or greater • Work requiring the disabling or bypassing safety interlocks *Any work within 10 feet of a non-insulated energized line*
4. Stored Energy (hydraulic, thermal, pneumatic, mechanical, etc.)	No stored energy	• Capable of being easily isolated; no disassembly required • LOTO	Required to disassemble system or piping to isolate energy (i.e., inserting blank flange)	
5. Confined Space Work	No confined space	Confined space (Class 1)	Confined space work (Class 2A and 2B)	Confined space work requiring permit (Class 2C)

ATTACHMENT 1, PAGE 4 OF 8

Table 1

Screening Guidelines for Work Planning & Control and Application of the Quality Graded Approach

	ESH&Q Risk Level			
Risk Category	**Negligible**	**Low**	**Moderate**	**High**
Quality Class (Optional)	**A4-Negligible**	**A3-Minor**	**A2-Major**	**A1-Critical**
ES&H Issues				
6. Excavation, Digging, Trenching or Concrete Penetration	None	• Excavations where no personnel will be in the trench • Dig depth of less than five feet	Excavations over five feet in depth with personnel using trench box "Aggressive concrete penetration	Excavations over five feet in depth where personnel will be working in trench and using engineered protective system (i.e., sloping or shoring)
7. Environmental Aspects/Impacts, refer to "Criteria for Significant Environmental Aspects"	No environmental aspects associated with work	Work has an environmental aspect but does not meet significance criteria	Work has an environmental aspect that meets significance criteria	Work has an environmental aspect that meets significance criteria and has potential for: (1) radiological release or (2) groundwater contamination or (3) regulatory violation
8. Work Requiring Respiratory Protection	Respiratory protection not required		Air purifying respirator required	Air supplied respirator required (SCBA or air line)
9. Non-Ionizing Radiation	None	• Exposure <TLV • Work with class I, II, IIIa, or lxia lasers	• Exposure >TLV • Work with class lamb or IIIb lasers	Pacemaker wearer or medical implant Work with class IV lasers

ATTACHMENT 1, PAGE 5 OF 8

Table 1

Screening Guidelines for Work Planning & Control and Application of the Quality Graded Approach

	ESH&Q Risk Level			
Risk Category	**Negligible**	**Low**	**Moderate**	**High**
Quality Class (Optional)	**A4-Negligible**	**A3-Minor**	**A2-Major**	**A1-Critical**
ES&H Issues				
10. Rigging and Heavy Lifting	None	Routine bucket truck, forklift, or crane work with trained personnel	• Lift is 75% or more of the rated capacity • Moving heavy loads by personnel other than riggers or qualified crane/fork operators	Critical lifts
11. Elevated Work	None	• No fall protection required • Work requiring fall protection equipment, but with establis hed procedures and qualification training (i.e., bucket truck use)	Work requiring fall protection equipment (i.e., harness, lanyard, etc.)	Work requiring a "Fall Protection Plan".
12. Work with OSHA Regulated Chemicals (i.e., Lead, Heavy Metals, etc.)	None	Below action level	Potential for exceeding action level	Potential for exceeding exposure level

Table 1

Screening Guidelines for Work Planning & Control and Application of the Quality Graded Approach

	ESH&Q Risk Level			
Risk Category	**Negligible**	**Low**	**Moderate**	**High**
Quality Classification	**A4-Negligible**	**A3 - Minor**	**A2 - Major**	**A1 - Critical**
Programmatic/ Quality Issues				
13. Stakeholder Perception	Negligible on over all DOE mission and program Protein crystallography experiments	Minor on over all DOE mission and program	Major on over all DOE mission and programs Biological level 1 experiments.	Critical on over all DOE mission and program Biological level 2 experiments
14. Data Integrity	Negligible reduction in data quality or equipment output Negligible reduction in data quality or equipment output. Data can readily be collected or reproduced with little or no need for additional resources, cost, and time is not a factor. e.g. An experiment runs for < 1 day period, and takes < 1 week to analyze the data. Experimental equipment used for data collecting needs to be calibrated and positioned correctly to avoid false data.	Minor reduction in data quality or equipment output Data can be collected or reproduced with the need of minor resources, costs, and time is a factor. e.g. An experiment runs for < 1 week and takes <1 month to analyze the data. It is important that experimental equipment used for data collecting is calibrated and positioned correctly to avoid false data.	Major reduction in data quality or equipment output Data can be collected or reproduced with the need of major resources, costs, and time is a major factor. e.g. An experiment runs for < 6 months and takes < 1 year to analyze the data. It is extremely important that experimental equipment used for data collecting is calibrated and positioned correctly to avoid false data.	Total loss/severe reduction in data quality or equipment output Data can or cannot be collected or reproduced without crucial res ources, costs, and time is a crucial factor. e.g. An experiment runs for >6 months and takes > 1 year to analyze the data. It is crucial that experimental equipment used for data collecting is calibrated and positioned correctly to avoid false data.

Table 1

Screening Guidelines for Work Planning & Control and Application of the Quality Graded Approach

	ESH&Q Risk Level			
Risk Category	**Negligible**	**Low**	**Moderate**	**High**
Quality Classification	**A4-Negligible**	**A3 - Minor**	**A2 - Major**	**A1 - Critical**
Programmatic/ Quality Issues				
15. Downtime of a Program	Negligible, e.g. • Less than two days • 2% of program schedule Negligible, e.g. • Less than 2 days • 2% of program schedule This would not apply to accelerator operations unless it was for only a few hours because the cost of the machine to operate on an hourly basis is somewhere around $2,000/hr. In 5 hours time it would already be equivalent to an A3 and that's not including labor and materials.	Minor, e.g. • Two days or more but less than four days • 2% or greater but less than 10% of program schedule A Proteus water switch used to protect a Dipole magnet may only take a few hours to repair/replace but could cause the machine to be down for several days in it fails.	• Major, e.g. • Four days or more but less than three weeks • 10% or greater but less than 30% of program schedule A vacuum bellows may only cost $1K but if the component fails, the accelerator can be down for weeks.	Critical, e.g. • Three weeks or more • 30% or greater of program schedule The active interlock system watches the beam position in the accelerators. If the beam position goes beyond a certain position, the beam will dump to protect the chamber and reduce the chances of elevated radiation levels. The machine could be down for more than a few weeks if system fails.

ATTACHMENT 1, PAGE 8 OF 8

Table 1

Screening Guidelines for Work Planning & Control and Application of the Quality Graded Approach

	ESH&Q Risk Level			
Risk Category	**Negligible**	**Low**	**Moderate**	**High**
Quality Classification	**A4-Negligible**	**A3 - Minor**	**A2 - Major**	**A1 - Critical**
Programmatic/ Quality Issues				
16. Equipment Dollar Loss	Negligible, e.g. • Less than $10K • Less than 2% of item/material or program cost e.g. Office supplies, office computers, furniture, fasteners and equipment not used for the accelerators or associated equipment unless there are numerous spares on hand and the equipment can be replaced with a quick turnaround.	Major, e.g. • 10K to 50K • 2% or greater but less than 10% of item/material or program cost e.g. Fasteners, machine equipment, and interlock components used for the accelerators and associated equipment, including network computers used to operate the machines. Note: A Proteus water switch used to protect a Dipole magnet may only cost $350, but this doesn't mean it would be an A4 just because of the dollar value. The cost to run the machine, labor for repair, and material needs to be factored in by the engineer.	Major e.g. • Greater than 50K to 250 K • 10% or greater but less than 50% of item/material or program cost e.g. Fasteners, equipment, interlock components, vacuum bellows used for the accelerators and associated equipment. A $100K Infrared microscope may not be categorized with an ESH&Q risk level of A2 because of the dollar value. The most expensive individual part in the system may cost $20K w/labor and the equipment is not needed to run the accelerator or experiment. Therefore it could be considered an A3.	Critical, e.g. • Greater than 250K • 50% or greater of item/material or program cost

ATTACHMENT 2, Page 1 of 2

DETERMINATION OF SINGLE OR MULTIPLE GRADED APPROACH PROGRAMS

The graded approach process may be applied in various levels at your site depending upon the complexity of the programs, facilities, and activities. It facilitates the implementation of the Nuclear Safety Management programs by using one of the following three options:

(1) one graded approach program, which encompasses all facilities/activities,
(2) individualized programs for each facility/activity for groupings of facilities/activities, or
(3) a combination of (a) and (b) for different programs.

Process Description

There are pros and cons for each of the three approaches as outlined below.

1) One Graded Approach Program
   a) Pros
      - The risk factors must be applied in a comprehensive fashion across all facilities/activities regardless of their preliminary hazard analysis
      - Easier to train staff
      - Process is easier to explain to stakeholders and customers
      - Makes it easy for rollup to corporate wide view
      - May reduce time for implementation
   b) Cons
      - Less flexible for individual program owners
      - May not fully take into account the unique risk management issues involved with individual facilities/activities
      - Precludes individual management participation
      - May increase the cost

2) Individualized programs for each facility/activity or groupings of facilities/activities
   a) Pros
      - Flexibility for individual project leaders to evaluate the unique risk management issues and appropriate controls for the work
      - Encourages continuous evaluation of the appropriate application of graded approach
      - Recognizes the same level of QA is not appropriate for all facilities/activities because of varying degrees of risks

   b) Cons
      - May lead to some inconsistent risk analysis based on individual groups own priorities

ATTACHMENT 2, Page 2 of 2

DETERMINATION OF SINGLE OR MULTIPLE GRADED APPROACH PROGRAMS

- Requires better defined boundaries which can ultimately eliminate flexibility
- May not be an effective use of resources due to time involved to analyze each item
- Additional training required for personnel involved in more than one program

3) Combination of a and b for different programs
   a) Pros
   - Allows for corporate broad application while allowing for activities within programs to be better defined for appropriate control of hazards/risks
   - Provides for ownership by project managers
   - Facilitates meeting customer requirements

   b) Cons
   - May lead to an inconsistent application of graded approach
   - Difficult to train staff
   - More difficult to describe to stakeholders/customers.

ATTACHMENT 3, Page 1 of 7

MISSION IMPORTANTANCE OR PROGRAMMATIC RISK

This attachment provides guidance for evaluating the mission importance or programmatic risk associated with a structure, system or component (SSC). The project engineer is to identify relevant criteria for upgrading any SSC graded lower than a performance grade (PG-3) to a PG-3. A recommendation to upgrade the SSC should be prepared by the engineer for review and concurrence by the Technical Review Board (TRB).

NOTE: Mission Important criteria are those that the engineer would use to evaluate any PG-4 or PG-5 SSCs to see if there is justification to recommend to the TRB that the SSC be upgraded to a PG-3 and may then come under Configuration Management.

This is an evaluation of all Stakeholder concerns, and the mitigating factors/programs that impact them. This final consideration is the heart of the TRB review, as it is the method by which the TRB assures themselves that a management override of the safety derived PG's is or is not warranted. Mitigating factors are such things as use of controlled procedures, standard practices, engineering or administrative controls, etc. Each identified Stakeholder concern should be addressed separately and completely, with the documented positions presented to the TRB.

<u>Situational/Circumstantial Considerations</u>

"What is the impact to this project or the site mission if this SSC fails to perform as intended?"

Components when used in the system that is determined to be high reliability dependent (i.e., maintenance intensive, difficult to obtain, or difficult to replace due to its location) should be upgraded.

- Will the failure of the SSC cause a reportable incident?
- Will the failure of the SSC cause public alarm and impact the mission?
- How will the failure of this SSC impact project cost or schedule?
- Will the failure cause the project to go through a restart?
- Are other activities using the same SSC?
- Will the failure of the SSC have an adverse effect on the performance requirements of a related PG-1, PG-2, PG-3, or PG-4 SSC?

ATTACHMENT 3, Page 2 of 7

MISSION IMPORTANTANCE OR PROGRAMMATIC RISK

Simplified Risk Assessment
Risk is a measure of economic loss or human injury. Risk reflects two aspects of failure: (1) the probability of the failure and (2) the consequence of the failure. Risk affects the success of a project.

The Simplified Risk Assessment Model is designed to answer three basic questions:

1. How do we identify and define risk in project execution?
2. How do we measure risk in the project?
3. How do we mitigate the defined and measured risk?

As a result of this calculation of risk factor, the engineer may reconsider the initial assignment of PG, and may elect to obtain consultation with other discipline experts to reconsider the initial PG and reassign a higher or lower PG.

APPLICATION OF THIS MODEL AT A DOE SITE

This risk assessment methodology is a highly simplified and subjective method; therefore, the engineer must use experience to rank the individual SSC for relative risk exposure.

THE METHODOLOGY

This method includes the calculation of three measures:
1. Probability of failure (P_F)
2. Consequence of failure (C_F)
3. Risk Factor (R_F)

Calculating the probability of failure

Magnitude is an arbitrary scale used to evaluate each attribute of risk.
Probability of Failure consists of three attributes: maturity, complexity, and dependency. The attributes of maturity and complexity have two sub-attributes – hardware and software.

MISSION IMPORTANTANCE OR PROGRAMMATIC RISK

Maturity Factor **(P_M)** is an evaluation of the SSC as to the state-of-the-art technology. If the component is known and "off-the-shelf," then it is assigned at a low risk factor or 0.1 magnitude. Conversely, if the component is a new design or requires R&D, then it would be assigned a high risk or 0.9 magnitude. Both hardware and software are evaluated similarly.

$P_M = P_{Mhw} + P_{Msw}$ where the subscript is the maturity of the software and hardware.

Complexity Factor **(P_C)** is a subjective evaluation of the complexity of the SSC, ranging from a simple design evaluation to an extremely complex design.

$P_C = P_{Chw} + P_{Csw}$ where the subscript is the complexity of the software and hardware.

Dependency Factor **(P_D)** is an overlooked attribute that requires careful review. The lowest risk factor is assigned to a SSC that is totally independent, and the highest risk factor is assigned to a SSC that is very dependent on existing SSC.

The Probability of Failure matrix lists various attributes and their respective risk magnitude. Therefore, the probably of risk is calculated using this equation:

$$P_F = (P_{Mhw} + P_{Msw} + P_{Chw} + P_{Csw} + P_D) / 5$$

<u>Consequence of Failure (C_F)</u>

Consequence of Failure (C_F) is the second component of the risk equation. This attribute consists of four factors: technical, cost, schedule, and public perception.

Technical Factor **(C_T)** is the consequences of the degradation of the SSC to perform its function.

Cost Factor **(C_C)** evaluates potential cost overruns in the application of the SSC.

Schedule Factor **(C_S)** evaluates the possible impact on the current schedule by the application of the SSC.

ATTACHMENT 3, Page 4 of 7

MISSION IMPORTANTANCE OR PROGRAMMATIC RISK

***Public Perception Factor* (C_P)** evaluates the consequences to the project due to public perception of the failure. This perception can range from indifference to outrage. The engineer must use diligence in assessing the public perception throughout the life cycle of the project. This factor is a real "look ahead" factor since the engineer must consider all possible scenarios of potential failures and how the media and public would react.

The Consequences of Failure matrix lists various attributes, and their respective magnitude. These four attributes are used in the equation for Consequences of Failure:

$$C_F = (C_T + C_C + C_S + C_P) / 4$$

Determining the Risk Factor (R_F) for the SSC

These two attributes are combined to establish the risk factor for each SSC:

$$R_F = P_F + C_F - P_F C_F$$

The SSC Simplified Risk Assessment page of this attachment is a suggested worksheet to organize assessments to calculate the risk factor.

USING THE RISK FACTOR WITH PERFORMANCE GRADING

The R_F is used to evaluate the risk of using each specific SSC in the project. The rationale used to establish the quantitative ranking is very subjective. This ranking is also used in a subjective manner to identify and reduce the risk factors that may lead to failure of mission-important projects. The application of the R_F is as follows:

a) If the R_F is less than 0.5, the PG of the SSC is appropriate and risk should be manageable with prudent project execution.

b) If the R_F is between 0.5 and 0.8, the risk is higher than desired and additional quality measures should be implemented, such as raising the PG to a higher level and closer involvement with QA and S&H organizations. The engineer should work closely with support organizations to manage the perceived risk to an acceptable level.

c) If the R_F is greater than 0.8, the SSC PG must be re-evaluated. This high risk factor requires that all possible techniques be considered to reduce or mitigate risk. Such techniques could include, for example, raising the PG of the SSC, planning and conducting more QA audits, using more rigorous review by the TRB. A Risk Mitigation Plan is highly recommended for SSC with high risk of failure.

ATTACHMENT 3, Page 5 of 7

MISSION IMPORTANT CONSIDERATIONS AND SIMPLFIED RISK ASSESSMENT

PROBABILITY OF FAILURE

Magnitude	Maturity Factor C_T		Complexity Factor C_F		Dependency Factor P_D
	Hardware PMhw	Software PMsw	Hardware PChw	Software PCsw	
0.1	Existing	Existing	Simple Design	Simple Design	Independent of Existing System, Facility, or Contractor
0.3	Minor Redesign	Minor Redesign	Minor Increase in Complexity	Minor Increase in Complexity	Schedule Dependent on Existing System, Facility, or Contractor
0.5	Major Change Feasibility	Major Change Feasibility	Moderate Increase	Moderate Increase	Performance Dependent on Existing System Performance, Facility or Contractor
0.7	Technology Available, Complex Design	New Software, Similar to Existing	Significant Increase	Significant Increase/Major Increase in No. of Modules	Schedule Dependent on Existing System Performance, Facility or Contractor
0.9	State of Art Some Research Complete	State of Art Never Done Before	Extremely Complex	Highly Complex Very Large Data Bases, Complex Operating Executive	Performance Dependent on New System, Facility or Contractor

* If one or more of the terms in the numerator are zero, reduce the denominator by an equal number of integers.

PROBABILITY OF FAILURE

$$P_F = (P_{Mhw} + P_{Msw} + P_{Chw} + P_{Csw} + P_D) / 5^*$$

ATTACHMENT 3, Page 6 of 7

MISSION IMPORTANT CONSIDERATIONS AND SIMPLFIED RISK ASSESSMENT

CONSEQUENCE OF FAILURE

Magnitude	Technical Factor C_T	Cost Factor C_C	Schedule Factor C_S	Public Perception Factor C_P
0.1	Minimal or No Consequences, Unimportant	Budget Estimate Not Exceeded, Some Transfer of Money	Negligible Impact on Program, Slight Development Schedule Change Compensated By Available Schedule Slack	No Public or Site Adverse Publicity
0.3	Small Reduction in Technical Performance	Cost Estimates Exceed Budget By 1 to 5 Percent	Minor Slip in Schedule (Less Than 1 Month) Some Adjustment in Milestone Required	Minor Public Awareness And Little Or No Public Or Media Attention
0.5	Some Reduction in Technical Performance	Cost Estimates Exceed Budget by 5 to 20 Percent	Small Slip in Schedule	Local Media Attention and Public Aware, FRESH Involved
0.7	Significant Degradation in Technical Performance	Cost Estimates Exceed Budget by 20 to 50 Percent	Development Schedule Slip in Excess of 3 Months	National Public Awareness and National Attention
0.9	Technical Goals Cannot Be Achieved	Cost Estimates Increase in Excess of 50 Percent	Large Schedule Slip That Affects Segment Milestones Or Has Possible Effects on Systems Milestones	Public Outrage, National Media Attention With Significant Negative Comments, DOE Show Cause of Stop Work

CONSEQUENCE OF FAILURE

$$C_F = (C_t + C_C + C_S + C_P) / 4$$

ATTACHMENT 3, Page 7 of 7

MISSION IMPORTANT CONSIDERATIONS AND SIMPLFIED RISK ASSESSMENT

SSC SIMPLIFIED RISK ASSESSMENT

SSC	P_{Mhw}	P_{Msw}	P_{Chw}	P_{Csw}	P_D	P_F Calculated	C_T	C_C	C_P	C_S	C_F Calculated	R_F Calculated

* The R_F calculated values provide the risk gradient, which requires subjective analysis following the guidelines provided in the narrative part of this Simplified Risk Methodology.

THE RISK FACTOR FORMULA:

$$R_F = P_F + C_F - (P_F C_F)$$

ATTACHMENT 4

FACILITY TECHNICAL BASIS AND AUTHORIZATION

Hazard Categorization (1)	**Nuclear Facility**	**Accelerator Facility (4)**	**Chemical Hazards Facility**	Radiological Facility	**Industrial Facility**	**Approval Authority (6)**
Technical Basis	DOE-STD-1027-92, Change Notice #1 **(2)**	DOE O 420.2	29 CFR 1910.119	DOE-STD-1027-92, Change Notice #1 **(2)** and Rad Con Posting Reference.	Default Categorization	BNL or BNL and DOE
Hazards Analysis (i.e., Technical Basis for Safety Limits)	SAR or BIO **(7)** (See DOE O 5480.23).	SAD (See DOE O 420.2).	Process Hazard Analysis (See 29 CFR 1910.119).	DOE O 440.1 Hazard Assessment and ES&H 1.3.3.	DOE O 440.1 Hazard Assessment and ESH Std 1.3.3	BNL or BNL and DOE
Safety & Operational Limits Documentation	TRS (See DOE 5480.22).	ASE (See DOE O 420.2) and Accelerator Safety Subject Area).	Process Hazard Analysis (See 29 CFR 1910.119).	Operational Safety Limits develop per ES&H Standard 1.3.4 and documented in FUA.	Operational Safety Limits developed per ES&H 1.3.4 and documented in FUA	BNL or BNL and DOE
Facility Authorization Envelope	DOE Authorization Agreement for Category 1 & 2 Facilities. **(3)**	DOE ASE Approval.	FUA	FUA	FUA	DOE & BNL for Nuclear and Accelerator BNL for Chem, Rad and Industrial
Safety Basis - DOE (Supporting Documentation for Facility Authorization Envelope)	SAR, TSR, and USQ processes, and Occurrence Reporting.	Accelerator Safety Assessment Document, Accelerator Safety Envelope, and USI.	Process Hazards Analysis.	Not required by DOE Orders.	Not required by DOE Orders	DOE
Safety Basis - BNL (Supporting Documentation for Facility Authorization Envelope)	FUA - Safety Basis Attached.	FUA Safety Basis Attached.	FUA	FUA with supporting safety/risk analysis.	FUA with supporting safety/risk analysis	BNL
Readiness Requirements	DOE ORR (See DOE O 425.1B).	DOE ARR (See DOE O 420.2).	ES&H Standard 1.3.2, Operational Readiness Review.	ES&H Standard 1.3.2, Operational Readiness Review.	ES&H Standard 1.3.2, Operational Readiness Review.	DOE & BNL for ORR and ARR BNL for RR
Configuration Control	USQ (See DOE O 5480.21). New rule issued 10CFR 830 1/10/01.	USI (See DOE O 420.2 and Accelerator Safety Subject Area).	ES&H Standards 1.3.5, 1.3.6 (modify FUA as incremental activities require).	ES&H Standards 1.3.5,1.3.6 (modify FUA as incremental activities require) **(5)**	ES&H 1.3.5/1.3.6 (modify FUA as incremental activities require)	DOE & BNL for USQ, BNL for USI and 1.3.5/1.3.6

1. **The Facility Hazard Categorization Subject Area determines the type of facility and subsequent documentation and approvals.**
2. **DOE-EM-STD-5502-94 is used in certain cases to supplement 1027-92, Change Notice #1 for Environmental Management facilities.**
3. **An Internal Authorization Agreement is required for Category 3 Nuclear Facilities (currently includes the Waste Management Facility).**
4. **The Accelerator Safety Subject Area gives detailed information specific to accelerators.**
5. **Exception: The Brookhaven Graphite Research Reactor (BGRR) is a radiological facility; however, it requires a USI process with DOE approval.**
6. **The BNL approval authority is the Deputy Director for Operations.**
7. **The Hazardous Waste Medical Facility (Category 2) operates under a Basis for Interim Operations.**