

Graded Approach Risk Level Matrix for Software

(Risk level classification is based on the potential consequence and the probability of that consequence occurring.)

Risk Level	Consequence of Software Failure
A1	<ul style="list-style-type: none"> • A death or serious injury (e.g., ORPS reportable: injury is immediately life-threatening or permanently disabling) • Off-site evacuation (public) • Compromise a limiting condition of operation • A reduction in the safety margin for a safety structures, systems, or components (SSCs) that is cited in DOE approved Documented Safety Analysis • A reduction in the safety margin for other systems such as toxic or chemical protection systems that are cited either (a) a DOE approved Documented Safety Analysis or (b) an approved hazard analysis per DOE P 450.1 and the DEAR ISMS clause • A non-conservative safety analysis, design, or misclassification of facilities or SSCs • >5 rem equivalent dose to an individual • Involves an environmental aspect that meets significance criteria, defined in the Environmental Aspects and Impacts Subject Area, and has the potential for (1) radiological release, (2) groundwater contamination, or (3) regulatory violation • A potential violation of regulatory requirements • ≥\$250,000 or ≥50% of item/material/program cost • ≥3 weeks program downtime or ≥30% of program schedule • Data integrity: Severe loss of, or severe reduction in, data quality or equipment output • A loss of any classified information (i.e., confidential National Security Information (NSI)/Restricted Data (RD) or above) • Public/Stakeholder impact that closes down an experiment or program or that has a critical impact on BNL/DOE mission or program
A2	<p>Does not meet the criteria in the risk level above but meets one of the following:</p> <ul style="list-style-type: none"> • Moderate injury (e.g., Days Away, Restricted or Transferred (DART)) • On-site evacuation (full/partial) • Safety management databases used to aid in decision making whose failure could impact safety SSC operation • Incorrect analysis, design, monitoring, alarming, or recording of hazardous exposures to workers or the public • Compromise the defense-in-depth capability of a nuclear facility • >1 rem or > Emergency Response Planning Guideline (ERPG)-1at site boundary for mitigated release ^{1&2} • ≥2 rem but ≤5 rem equivalent dose to an individual ³ • Involves an environmental aspect that meets significance criteria defined in the Environmental Aspects and Impacts Subject Area • ≥\$50,000 or ≥10% of item/material/program cost • ≥4 days program downtime or ≥10% of program schedule • Data integrity: Major loss of, or major reduction in, data quality or equipment output • A loss of any DOE sensitive information • Public/Stakeholder impact that brings the experiment to the attention of the community and activist groups or have a major impact on BNL/DOE mission or program

Graded Approach Risk Level Matrix for Software

(Risk level classification is based on the potential consequence and the probability of that consequence occurring.)

A3	<p>Does not meet the criteria in the risk levels above but meets one of the following:</p> <ul style="list-style-type: none"> • Minor injuries, (e.g., first aid or recordable) • ≥ 100 mrem but < 2 rem equivalent dose to an individual⁴ • Affect environment, safety, health monitoring or alarming systems • Affect the safe operation of SSCs • Involves an environmental aspect but does not meet significance criteria defined in Environmental Aspects and Impacts Subject Area • $\geq \\$10,000$ or $\geq 2\%$ of item/material/program cost • ≥ 2 days program downtime or $\geq 2\%$ of program schedule • Data integrity: Minor loss of, or minor reduction in, data quality or equipment output • Loss of information that is not authorized by DOE for public release • Public/Stakeholder impact that is below public perception or have a minor impact on BNL/DOE mission and program
A4	Does not meet the criteria in the risk levels above

¹ EPA Protective Action Guide (PAG): US EPA, Office of Radiation Programs, Manual of Protective Action Guides and Protective Actions for Nuclear Incidents (400-R92-001)

² Emergency Response Planning Guideline (ERPG) values are intended to provide estimates of concentration ranges where one reasonably might anticipate observing adverse effects as described in the following definitions as a consequence of exposure to the specific substance. See: American Industrial Hygiene Association, *2004 Emergency Response Planning Guidelines (ERPG) Update Set* (Stock number: AEAR04-561).

- The ERPG-1 is the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hr without experiencing other than mild transient adverse health effects or perceiving a clearly defined, objectionable odor.
- The ERPG-2 is the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hr without experiencing or developing irreversible or other serious health effects or symptoms which could impair an individual's ability to take protective action.
- The ERPG-3 is the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hr without experiencing or developing life-threatening health effects.

³ Federal law violation.

⁴ ORPS trigger