Department of the Army Pamphlet 385–30

Safety

Risk Management

Headquarters
Department of the Army
Washington, DC
2 December 2014

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 385–30
Risk Management

This major revision, dated 2 December 2014--

- Clarifies the applicability of this pamphlet (para 1-5).
- Introduces DD Form 2977 (Deliberate Risk Assessment Worksheet) and rescinds DA Form 7566 (Composite Risk Management Worksheet) (now obsolete) (para 1-8).
- Updates and clarifies the requirements and terminology for deviations from Army safety standards (paras 1-8*e*, 4-5, and 4-6).
- Updates table on severity and risk acceptance authority (table 3-2).
- Clarifies the documentation requirements for risk acceptance (paras 4-5 and 4-6).
- Provides updated instructions for DA Form 7632 (Deviation Approval and Risk Acceptance Document (DARAD)) (para 4-6 and app C).
- Provides appendices containing guidance on the integration of risk management into the areas of Army learning and policy systems, sexual harassment and assault prevention, private motor vehicle accident prevention, and suicide prevention (apps D and E).
- Updates definitions in accordance with Army Techniques Publication 5-19 (glossary).
- Incorporates doctrinal changes in Army Techniques Publication 5-19 (throughout).
- Makes administrative changes (throughout).

Headquarters
Department of the Army
Washington, DC
2 December 2014

*Department of the Army Pamphlet 385–30

Safety

Risk Management

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army

History. This publication is a major revision.

Summary. This pamphlet provides information needed to carry out policies and procedures prescribed by AR 385–10. It is designed to assist users in implementing and integrating risk management into all phases of the Army operations.

Applicability. This pamphlet applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this pamphlet is the Director of the Army Staff. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include a formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Army Safety Office (DACS–SF), Building 1456, 9351 Hall Road, Fort Belvoir, VA 22060–5527.

Distribution. This publication is available in electronic media only and is intended for command levels C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This pamphlet supersedes DA Pam 385–30, dated 10 October 2007.

UNCLASSIFIED

Contents—Continued

Contents—Continued

Glossary

Chapter 1
Risk Management

1–1. Purpose

This pamphlet establishes a framework for making risk management a routine and required part of planning, preparing, and executing missions and everyday tasks in accordance with Department of Defense Instruction (DODI) 6055.1 and Army Regulation (AR) 385–10. This framework allows Army leaders to operate with maximum initiative, flexibility, and adaptability. Army operations, whether they involve military situations including tough, realistic training, combat operations, contingency basing, or the industrial base supporting research, development, testing, and production, are demanding and complex. They are all inherently dangerous and each has the potential to jeopardize Soldiers and Army civilians, resulting in the needless loss of limited resources. Managing risks related to such operations requires educated judgment, situational knowledge, demonstrated experience, and professional competence. The risk management process enables Army leaders to make informed, conscious decisions to accept risk involving safety and occupational health and other risk factors. For detailed techniques on implementation of risk management in the operational environment, see Army Techniques Publication (ATP) 5–19. ATP 5–19 provides doctrinal guidance on managing risk within the conduct of operations. This pamphlet and ATP 5–19 are designed to be complimentary, and in tandem, they provide guidance on the implementation of risk management throughout the Army.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this pamphlet are explained in the glossary.

1–4. Introduction

a. Unidentified and unmanaged hazards and their associated risks impede successful Army missions, undermine readiness, decrease morale, and deplete resources. The holistic approach of risk management provides commanders a tool to recognize, evaluate, eliminate, and control the diverse threats and risks to mission execution. The underlying philosophy of risk management is that a loss is a loss. The loss can be any one of the following:

(1) Tactical (threat-based) loss.

(2) Accidental (hazard-based) loss.

(3) Loss due to terrorism, suicide, homicide, illness, or substance abuse.

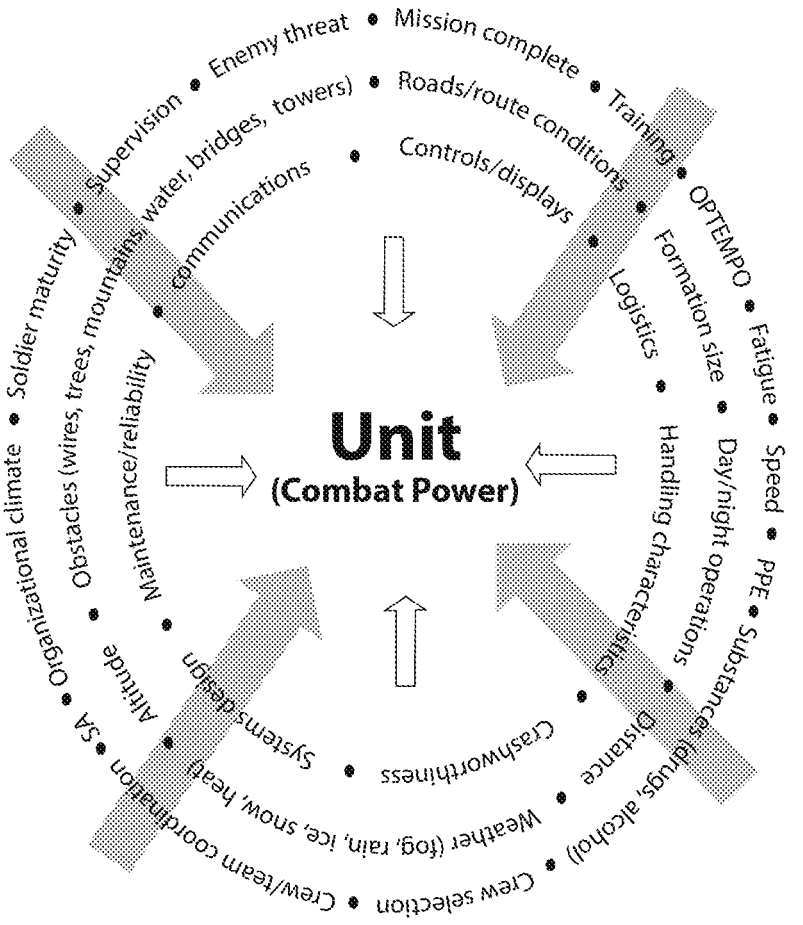
b. Any event that threatens combat readiness and the ability to project power can and should be considered a risk factor.

c. Army leadership and management at every level need to exercise risk management. As shown in figure 1–1, due to the holistic nature of risk management, the process requires multidisciplinary participation using a range of diverse tools to provide the commander with the knowledge to make informed risk decisions about all the identified hazards and their risk. Losses caused by accidents are a major threat to combat readiness. Practitioners use risk management to identify, evaluate, and manage risks to missions, personnel, equipment, facilities, and the environment during peacetime, contingency operations, and wartime due to safety and occupational health and other risk factors.

d. Risk management provides consistent and systematic identification and communication of risks, consequences, and potential actions to mitigate those risks to the appropriate commander for an acceptance decision.

e. Safety standards and policy cannot cover every Army mission and operation. Use of risk management allows commanders the operational flexibility required to make informed decisions.

f. A properly documented risk assessment serves as evidence that command decisionmaking was based on sound judgment and reasonable principles and aids in defense of negligence claims against the Army by practicing due diligence.



Legend for Figure 1–1;
SA — situational awareness
PPE — personal protective equipment
OPTEMPO — operating tempo

Figure 1–1. Holistic approach of risk management

1–5. Applicability

In accordance with AR 385–10, Army leaders will integrate risk management into all aspects of military missions and operations, industrial planning, research and development, systems, equipment, procurement, testing, construction, and processes to increase efficiency and effectiveness by eliminating or controlling adverse and risky conditions that will degrade their execution and value to the Army. Risk management will be applied to Soldiers, Army civilians, and the total life cycle of missions, systems, operations, equipment, and facilities, from conception to completion or disposal.

a. The basic concepts of risk management apply to all Army operations and functional areas. However, the methodology for evaluating and executing the military decisionmaking process and troop leading procedures has been established under ATP 5–19. Tools and techniques found in this pamphlet are available to support ATP 5–19 analyses and decisionmaking. Guidance for the application of risk management to Army learning systems, leadership, sexual harassment and/or assault prevention, suicide prevention, and private motor vehicle (PMV) accident prevention is provided in appendices E and F of this pamphlet.

b. The Army Acquisition Community risk assessment and acceptance processes are contained in AR 70–1, Military Standard (MIL–STD)-882, and Department of the Army Pamphlet (DA Pam) 385–16. The Army has established several weapon system related safety review boards, such as the Army Weapon System Safety Review Board (AWSSRB), the Army Fuze Safety Review Board, the Ignition System Safety Review Board, and the U.S. Army Aviation and Missile Command Software Safety Review Board, to assist acquisition program managers (PMs) in the evaluation and management of the risks associated with their systems.

c. Deviations from range standards and procedures are addressed in AR 385–63 and DA Pam 385–63.

d. Facility design and construction will apply the risk management principles contained in DA Pam 385–16.

e. AR 95–1 governs flight operations. Commanders will integrate risk management into aviation mission planning and execution at every level. Commanders will establish a training and certification program to ensure standardization and understanding of the mission approval and risk management for all personnel. Commanders will develop local briefing checklists and risk assessment worksheets for use in assessing aircrew mission planning and risk. Guidance on risk management is contained in Technical Circular 3–04.11, Army Doctrine Publication (ADP) 5–0, ATP 5–19, and AR 385–10.

f. When Army units, facilities, or operations are tenants on another Service's or allied nation's installation or are subordinate to another Service's or allied nation's lead during Joint operations, Army risk management must include Joint and/or multi-national risk management methodology considerations. Joint operations at non-enduring locations will use the process and procedures in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 4360.01 for deviations from ammunition and explosives (AE) or chemical agent safety standards (see para 4–6).

1–6. The principles of risk management

The four principles of risk management are—

a. Integrate risk management into all phases of missions and operations.

b. Make risk decisions at the appropriate level.

c. Accept no unnecessary risk.

d. Apply risk management cyclically and continuously.

1–7. Hazard versus risk

a. Hazard is a condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. Therefore, a hazard can have several possible negative outcomes or losses (for example, injury, death, damage, mission failure, mission degradation, increased resource(s) expenditures, and adverse public relations).

b. Risk is determined after hazards are identified and analyzed and is presented as a combined expression of loss probability and severity.

1–8. Risk management

a. Risk management is the Army's primary process for assisting organizations and individuals in making informed risk decisions in order to reduce or offset risk, thereby increasing effectiveness and the probability of mission success. It is a systematic, cyclical process of identifying and assessing hazards, then mitigating the associated risks. It is the responsibility of all commanders, staff, leaders, Soldiers, and Army civilians to integrate risk management into all planning and operations.

b. The process consists of the following five steps (see figure 1–2):

(1) Identify the hazards.

(2) Assess the hazards.

(3) Develop controls and make risk decisions.

(4) Implement controls.

(5) Supervise and evaluate.

c. The risk assessment consists of the first two steps of the risk management process. In step 1, individuals identify the hazards that may be encountered in executing an activity. In step 2, they determine the impact of each hazard on the activity. The risk assessment provides for enhanced situational awareness. This awareness builds confidence and allows Soldiers, units, Army civilians, and organizations to implement timely, efficient, and effective protective control measures.

d. Steps 3 through 5 are the essential follow-through actions to manage risk effectively. In these steps, leaders balance risk against costs and take appropriate actions to eliminate unnecessary risk and accept residual risk at the appropriate level. During execution, leaders continuously assess the risk to the overall mission and to those involved in the task. Finally, leaders and individuals evaluate the effectiveness of controls and provide lessons learned so that others may benefit from the experience.

e. Risk assessments, with the exception of deviations from AE or chemical agent safety standards, will be documented using DD Form 2977 (Deliberate Risk Assessment Worksheet). Instructions for DD Form 2977 can be found in appendix B. DA Form 7632 is mandatory for deviations from AE or chemical agent safety standards. Instructions for DA Form 7632 can be found in appendix C.

1–9. Compliance and risk management

a. Risk management provides commanders with the ability to balance risk levels with other desired outcomes in terms of impact to mission, cost, performance, and schedules. Risk management does not give the Army the authority to violate or deliberately disobey local, state, national, or host nation laws: commanders cannot use the process to

justify ignoring regulatory restrictions, such as occupational safety and health regulations, life safety, and fire protection codes, physical security requirements, or to alter or bypass legislative intent. However, when restrictions imposed by other entities adversely affect the mission, planners may use risk management to develop alternate courses of action (COAs) that still conform to legal requirements and require approval at the appropriate level of leadership.

b. Risk management assists the commander in complying with regulatory and legal requirements by—

(1) Identifying applicable legal standards that affect the mission.

(2) Identifying alternate COAs or alternate standards that meet the intent of the law.

(3) Ensuring better use of limited resources by establishing priorities to correct known hazardous conditions that will result in the highest return on investment.

(4) Documenting their deviations from non-statutory regulations using DD Form 2977 (and, as applicable, DA Form 7632).

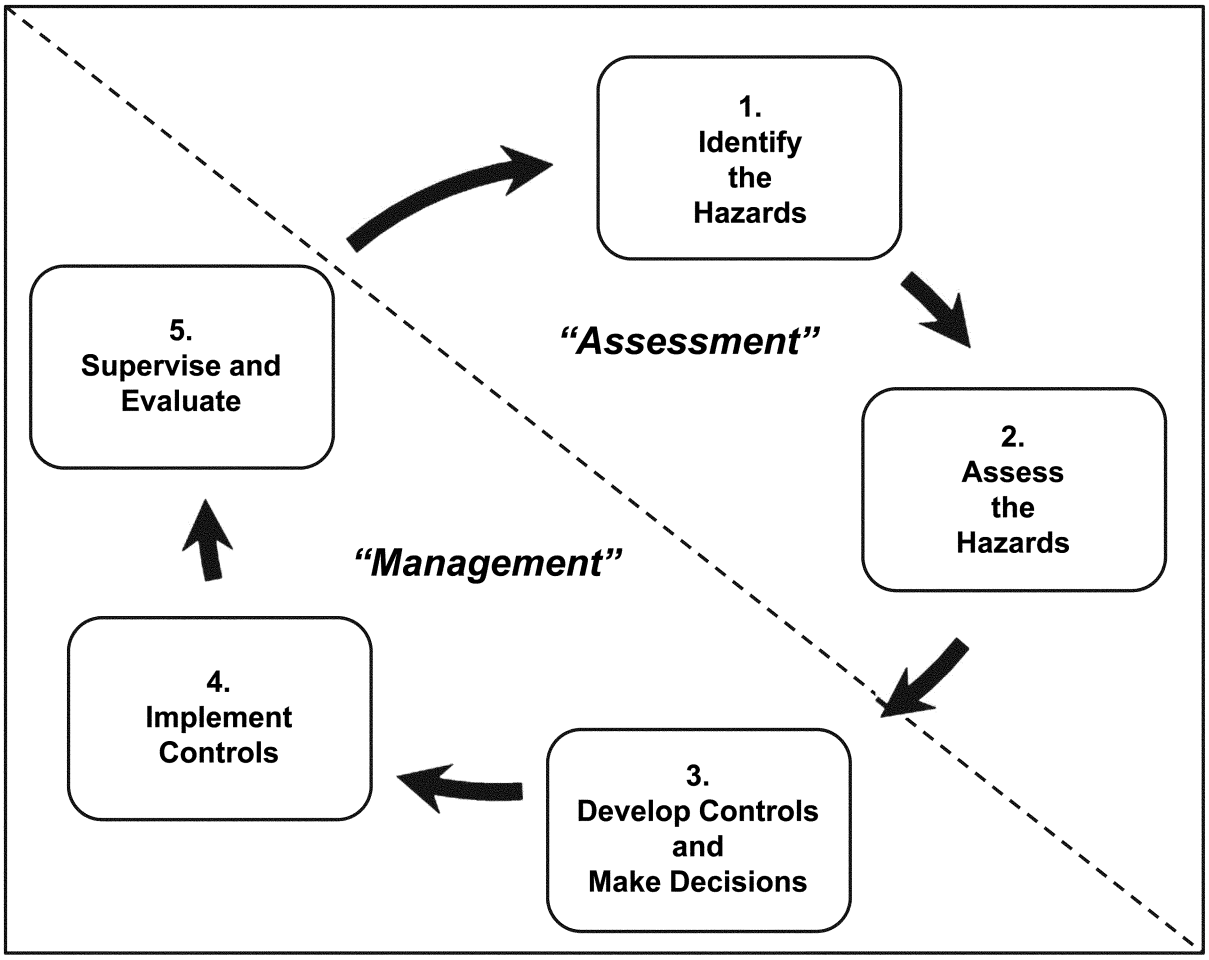


Figure 1–2. Five-step cycle of risk management

Chapter 2
Step 1 – Identify the Hazards

2–1. Introduction

The first step in risk management is to identify the hazards associated with a task and/or subtask, operation, process, facility, or equipment. DD Form 2977 is an effective tool for systematically documenting the identification of hazards.

2–2. Defining limits and tasks

a. Before beginning hazard identification the limits of the assessment must be defined. For example, determine the scope of the tasks and/or subtasks, operations, processes, facilities, equipment, and so forth, of the mission or overall task to which risk management is being applied. The purpose of defining limits is not to ignore hazards, but rather to clearly define what is being analyzed. This allows the assessor to focus on those hazards associated with the event and not on other hazards that have no relationship to it. Those unassociated hazards should be addressed by another risk assessment. As an example, if the analysis were being conducted of a vehicle repair operation, then the limits of the analysis would be stated as the garage area or even as just bay 1 in the garage area. The assessor would only consider those hazards that might be present in bay 1 and would not look at identifying possible hazards on the driveway coming into the bay or on the street outside.

b. Once the limits are defined, the tasks (and, as appropriate, facilities and equipment) will be listed. A task analysis will aid in identifying hazards and may also serve as a tool for developing standing operating procedures (SOPs).

c. DD Form 2977 is formatted in a manner that is conducive to defining the limits and tasks of the assessment.

2–3. Hazard identification methods and tools

Hazards are most effectively described when the following three components are addressed: source, mechanism, and outcome. When identifying hazards, consideration should be given to these three elements to ensure the relationships between hazards and mishaps are recognized. There are numerous methods for identifying hazards ranging from visual inspections to test and engineering analysis and predictive scenarios. Hazard identification works best when performed as a team effort with input and expertise from impacted operators and/or workers, safety and occupational health professionals such as explosives safety specialists and health physicists, and others such as engineers and scientists.

a. A visual inspection provides a rudimentary, but effective, means of identifying existing hazards and sources of potential hazards.

b. Accident reports can contain a wealth of information regarding hazards. Accident reports may address sub-systems or sub-elements of a task or the system or task in its entirety. When identifying hazards for a system (sub-system) or task (sub-elements) it is often advantageous to collect as much accident information as possible and then conduct trend analyses for the system or task under consideration.

c. Hazard reports, hazard analyses, defect reports, engineering change proposals, and analogous reports on the system or activity under consideration and similar or related systems or activities are great sources of information. As with accident reports, when identifying hazards for a system or task it is often advantageous to collect as much accident and hazard-related information as possible and then conduct trend analyses for the system or task under consideration.

d. Technical publications (for example, guides, studies, consensus standards, and so forth) from professional societies, Government organizations, industry, or academia can provide valuable assistance to hazard identification.

e. Engineering analysis of materials, systems, processes, and human interfaces can be used to identify potential hazard sources and failure modes. In addition, it may be advantageous to conduct destructive or non-destructive testing on systems and/or sub-systems to gather data that can aid in identifying and assessing failure modes and hazards.

f. Operator's manuals, safety data sheets, and hazard checklists and/or reference lists provide generic consolidated historical hazard information. Since these are generic (for example, they do not consider operator and facility and/or environmental specific factors) it is not suggested that they be used as the sole means of identifying system and/or activity hazards, but they are often beneficial for starting the hazard identification process.

g. Predictive scenarios, especially when combined with the above-listed methods and tools, provide the most comprehensive, system- and/or situation-specific means of identifying hazards. Predictive scenarios can range from "brain-storming" hazard scenarios to system mock-up and activity simulation. A "crawl-walk-run" approach should be taken including hazard assessment along the way.

Chapter 3
Step 2 – Assess the Hazards

3–1. Assessing the hazards

Step 2 involves evaluating each hazard and assigning a level of risk based on the estimated probability and severity. Risk always deals with uncertainty; it involves estimating future losses, for which neither the likelihood nor impact on mission, Soldiers, Army civilian personnel, the public, equipment, systems, or the environment is known with certainty.

3–2. Definitions

a. Risk. Risk is defined as the probability and severity of loss linked to hazards. It is simply the measure of the expected loss from a given hazard or group of hazards, usually estimated as the combination of the likelihood (probability) and consequences (severity) of the loss.

b. Probability. An approximation of the likelihood of a hazard scenario or mishap occurring. Probability is assessed as frequent, likely, occasional, seldom, or unlikely.

c. Severity. An approximation of the amount of potential harm, damage, or injury associated with a given mishap.

d. Residual risk. The risk associated with a hazard that remains after implementing all planned countermeasures or controls to eliminate, reduce, or control the impact of the hazard. The residual risk may be equal to the initial risk, especially when the initial risk was so low that the hazard did not warrant expenditure of funds to mitigate.

3–3. Probability

Probability is the basis of the likelihood of something happening. In risk management, probability refers to an approximation of the likelihood of a hazard scenario or mishap occurring. The likelihood of an event can range between 0 and 1.0. Zero represents an event that cannot possibly occur. A probability of 1.0 indicates an event that always occurs.

a. For a probability to be meaningful, an exposure interval must be associated with it. The exposure interval can be a unit of time; an activity, such as, miles driven, aircraft landings, operations, machine cycles, units produced; or the life cycle of the facility, equipment, or process.

(1) Normally, the life cycle for a building is 25 years; special purpose facilities may have a greater or shorter life cycle.

(2) For equipment, the life cycle is considered 10 years except for electronic equipment, which can have a very short life cycle.

b. Probabilities are estimations. The better the knowledge of the situation, the more factual and historical information used, and the greater the experience of the evaluator, the more accurate the estimation will be. Except in extremely technical evaluation, the probabilities should be considered as falling within a range.

c. In the real world, it is often very hard to determine objective or numerical probability values. The information necessary to derive these values is often missing, or more often than not, there is just not enough time to make the necessary studies. When the information and time are available, an effort should be made to use the numerical probability values. However, in the other situations it becomes necessary to make estimates based on available knowledge. To aid evaluators, probability ranges have been established using keywords and phrases to help estimate the likelihoods for the occurrence of a hazard scenario or mishap. Table 3–1 shows these probability ranges.

Table 3–1.
Risk management probability categories

Probability	Symbol	Definition
Frequent	A	Continuous, regular, or inevitable occurrences
Likely	B	Several or numerous occurrences
Occasional	C	Sporadic or intermittent occurrences
Seldom	D	Infrequent occurrences
Unlikely	E	Possible occurrences but improbable

3–4. Severity

Severity approximates the amount of potential harm, damage, or injury associated with a given mishap occurring. It is the second of two risk components.

a. Severity and probability are independent of each other. In other words, determining severity has no relationship to determining the probability.

b. It is often hard to determine an objective amount or cost of a mishap outcome. Therefore, severity ranges have been established to aid in this process. They delineate a range of mishap outcomes similar to the probability ranges. They are shown in table 3–2.

c. Once more, the recommended procedure is to start at the top and work down the table, selecting the range representing the maximum credible damage or loss.

d. When selecting, the assessor must consider the impact on the mission, possible human loss, and equipment or system damage. For instance, an accident might not result in any injuries but a simple piece of equipment, worth only a few hundred dollars, is damaged. While this might be classified as marginal from standpoint of human and equipment loss, its loss could result in having to cancel the mission, task, and job.

Table 3–2.
Risk management severity categories

Severity	Symbol	Quantitative value — Injury or Illness[1]	Quantitative value — Dollars[1]	Definition
Catastrophic	I	1 or more death or permanent total disability	Loss equal to $2 million or more	Death, unacceptable loss or damage, mission failure, or unit readiness eliminated
Critical	II	1 or more permanent partial disability or hospitalization of at least 3 personnel	Loss equal to or greater than $500 thousand but less than $2 million	Severe injury, illness, loss, or damage; significantly degraded unit readiness or mission capability
Moderate	III	1 or more injury or illness resulting in lost time	Loss equal to or greater than $50 thousand but less than $500 thousand	Minor injury, illness, loss, or damage; degraded unit readiness or mission capability
Negligible	IV	1 or more injuries or illnesses requiring first aid or medical treatment	Loss less than $50 thousand	Minimal injury, loss, or damage; little or no impact to unit readiness or mission capability

Notes:
[1] Quantitative values are based on definitions for Class A through D accidents. See AR 385–10.

3–5. Matrices

Table 3–3 is an expression of the Army's standard risk matrix, as found on DD Form 2977 and within ATP 5–19. Table 3–3 shows conversion of probability and severity into both a specific risk level and corresponding risk assessment code. This assessment is an estimate, not an absolute. It may or may not be indicative of the relative danger of a given operation, activity, or event. The levels of risk are listed in table 3–4.

a. Extremely high risk. Loss of ability to accomplish the mission or the mission produces extremely severe outcomes. This implies that the risk associated with this mission, activity, or event may have severe consequences beyond those associated with this specific operation or event. The decision to continue must be weighted carefully against the potential gain to be achieved by continuing this COA.

b. High risk. Significant degradation of mission capabilities in terms of the required mission standard, inability to accomplish all parts of the mission, high potential for serious injury to personnel, or inability to complete the mission to standard, if hazards occur during the mission. This implies that, if a hazardous event occurs, serious consequences will occur. The decision to continue must be weighted carefully against the potential gain to be achieved by continuing this COA.

c. Medium risk. The ability to complete the mission will be slightly degraded in the event this hazard occurs. If a hazardous event occurs, it will only slightly impact on the mission, result in only minor injury or loss, and not affect overall readiness.

d. Low risk. Expected losses have little or no impact on accomplishing the mission. Injury, damage, or illness will be minor and have no long-term impact or effect.

Table 3–3.
Standardized Army risk matrix

		Probability (expected frequency)				
		Frequent: Continuous, regular, or inevitable occurrences	**Likely: Several or numerous occurrences**	**Occasional: Sporadic or intermittent occurrences**	**Seldom: infrequent occurrences**	**Unlikely: Possible occurrences but improbable**
Severity (expected consequence)		A	B	C	D	E
Catastrophic: Death, unacceptable loss or damage, mission failure, or unit readiness eliminated	I	EH	EH	H	H	M
Critical: Severe injury, illness, loss, or damage; significantly degraded unit readiness or mission capability	II	EH	H	H	M	L
Moderate: Minor injury, illness, loss, or damage; degraded unit readiness or mission capability	III	H	M	M	L	L
Negligible: Minimal injury, loss, or damage; little or no impact to unit readiness or mission capability	IV	M	L	L	L	L

Legend for Table 3-3.:
EH – extremely high risk
H – high risk
L – low risk
M – medium risk

Table 3–4.
Risk matrix codes and descriptions

Symbol	Risk Assessment Code (RAC)	Description
EH	1	Extremely High
H	2	High
M	3	Medium
L	4	Low

3–6. Maximum credible risk

Maximum credible risk is the risk associated with the hazard that is the most severe and the most credible. This is the most commonly used summation method. It is possible in a given analysis that several risks of the same magnitude would be identified. For instance, during analysis of a process, the assessor identified 2 extremely high, 7 high, 5 medium, and 26 low risks. In this example, one of the two extremely high risks events would be the maximum credible risk. To decide which, the following should be considered:

a. The one with the greatest severity would be used as maximum credible risk.

b. If the severities are the same, then the one with the greatest probability should be used. If severity and probability are the same for both, additional hazard analysis techniques should be used to identify the maximum credible event - the most disastrous maximum credible loss identified for a given system or operation.

3–7. Other matrices.

a. The risk matrix and associated probability and severity definitions prescribed in MIL–STD–882 differ from those defined in this pamphlet and are applicable to the Army Acquisition Community for use in the systems engineering process (see also para 1–5*b*). DODI 5000.02 defines the risk acceptance authorities for these applications. These standards allow for the use of alternate, tailored probability and severity definitions and risk matrices when formally approved (see AR 70–1 and DA Pam 385–16).

b. Differing risk matrices and probability and severity definitions may be used by other Services and nations with which the Army routinely partners. Paragraph 1–5*f* provides guidance for reconciling these differences during Joint and multi-national operations.

Chapter 4
Step 3 – Develop Controls and Make Risk Decisions

4–1. Develop controls and make risk decisions

Step 3 is made up of two sub-steps.

a. Substep 1–Develop controls. After assessing each hazard, the assessor develops one or more controls that either eliminate the hazard or reduce the risk (probability or severity) of a hazardous incident. When developing controls, the assessor considers the reason for the hazard (that is, the root cause), not just the hazard itself.

b. Substep 2–Make risk decisions. Risk decisionmaking involves determining whether the residual risk is justified. The decision maker decides whether controls are sufficient and acceptable and whether to accept the resulting residual risk. If the decision maker determines the residual risk level is too high, the decision maker can direct the development of additional controls or alternate controls, or the decision maker can modify, change, or reject the COA.

4–2. Developing controls

a. Chapter 3 (step 2) provides guidance for assessing hazards and analyzing their sources, mechanisms, and outcomes. Once these elements of the hazard are understood, various controls and countermeasures should be developed. In this step of risk management, the idea is to brainstorm as many controls and countermeasures as possible.

b. Once a list of possible controls has been developed for each hazard, the next step is to evaluate them. The selection of the best control measures should be made based on the risk control hierarchy, effectiveness in mitigating the risk (that is, the resultant residual risk), cost, feasibility, and required level of support and/or supervision. Apply the following hierarchy to risk control selection:

(1) Elimination;

(2) Substitution of less hazardous materials, processes, operations, or equipment;

(3) Engineering controls;

(4) Warnings;

(5) Administrative controls;

(6) PPE. PPE will be used only after a hazard assessment meeting requirements of subpart 1910.132 of Title 29, Code of Federal Regulations has been completed and:

(a) Engineering or management controls are not feasible or do not sufficiently eliminate the hazard; or,

(b) Development or installation of engineering controls are pending; or,

(c) For short-term, non-routine operations, for which engineering controls are not practical or for emergencies (for example, spills, including cleanup operations), malfunctions, emergency egress, and damage-control activities.

4–3. Residual level of risk

a. After identifying effective controls, the risk assessor returns to the risk assessment matrix to determine the residual level of risk for each hazard and the overall residual risk for the operation. The process of analyzing the hazards and proposing options to reduce or eliminate them should be repeated until the most effective controls have been identified. Even though some proposed controls do not significantly lower the risk level of a given hazard, they should be implemented if their benefits outweigh the costs of implementation.

b. The appropriate level of command must approve the mission, making a final risk decision based on the residual level of risk. The overall residual level of risk combines the residual level of risk for all identified hazards. The residual level for each hazard may differ. The overall residual level will be equal to or higher than the highest residual level for each hazard. The responsible individual must consider the number and type of hazards present. In some cases, for example, a commander may determine that the overall residual level of risk is higher than any one hazard. The assessment could be based on a number of lower-risk hazards, if in combination they present a higher risk. For example, commanders may determine that a mission risk assessment should have medium risk level even when all hazards have a low residual level. Based on the complexity of required controls and the potential synergistic effect of

all hazards, a commander may determine the level of risk for a mission is high when the residual level for the individual hazards ranges from low to medium.

4–4. Making risk decisions

Once the potential countermeasures and controls have been developed, risk decisions need to be made. This involves deciding which countermeasures to use and accepting residual risks.

a. The decision to select countermeasures and controls can often be made at the lowest echelons, by the immediate leader, designer, or process developer. However, when the hazard is not eliminated or controlled to tolerable limits, Army leadership needs to decide about the acceptability of the risk based upon mission requirements. Accepting risk is a serious matter; therefore, the appropriate level of Army leadership must weigh the increased danger to the mission, personnel, equipment, public, property, and environment against the operational requirement that necessitated acceptance of a significant level of risk. As a decisionmaking tool, risk management is effective only when the information is passed to the appropriate level of command for decision.

b. The appropriate risk acceptance authority is typically determined by three factors: the duration of the risk, the level of risk, and the ownership of the resources necessary to control, eliminate, or correct the hazard in an appropriate time frame. The exposure of unrelated personnel to risk and the resultant level of required coordination may also affect the required level of risk acceptance (for example, the exposure of host nation facilities to risk from an Army operation).

c. Army headquarters commanders are required to establish and publish approval authority for risk acceptance and decisionmaking for their command or adopt, in writing, table 4–1 of this pamphlet.

d. The duration of the risk is the total length of time that the mission, personnel, equipment, property, or environment will be exposed to the hazard. When determining the required risk acceptance level in table 4–1, the duration of the risk will not be divided into shorter increments to lower the risk acceptance authority level. Consideration must be given to whether the mission is recurring or nonrecurring.

(1) *Recurring missions*. Recurring missions are operations that are cyclic in nature, are anticipated to occur again in the near future, and involve the same hazards, control measures, and risks during each occurrence, such as night-training flights, rifle-range training, and so forth. For recurring missions, the duration should be based on the anticipated total time period to accomplish all recurring missions; for example, if the mission will be conducted for 1 week every month for 3 years, then the duration used would be 3 years, not 1 week or 1 month.

(2) *Nonrecurring missions*. Nonrecurring missions are missions that are not anticipated to occur again in the near future. Normally, these types of operations occur during contingencies, wartime conditions, or other unique situations.

e. The level of authority accepting the potential consequences of a given hazard is determined by the level of residual risk associated with that hazard, mission, or event. The greater the risk and longer the duration the higher that decision must be elevated. In organizations led by Army civilian leaders, equivalent civilian grades may be substituted for military ranks; see table 4–2.

f. Risk can only be accepted by the commander with the resources and/or authority necessary to control, eliminate, or correct the hazard in an appropriate timeframe. When unrelated personnel, facilities, or equipment are exposed to a hazard, the appropriate authority in the exposed organization will acknowledge the hazard and accept the risk to their personnel, facilities, or equipment. On Army installations the installation commander holds ultimate responsibility for all risk on the installation and must be made aware and acknowledge the risk prior to acceptance. Coordination will be made with all units that are exposed to this risk. The most common scenario is when the risk is due to the operations of one organization (for example, a tenant on an installation), but exposes other organizations' personnel, facilities, or equipment to hazards. In this case, the other affected organizations (for example, the garrison commander and the installation commander) must be made aware and acknowledge the risk prior to risk acceptance by the organization creating the risk. Examples would include the risk associated with explosives arcs exposing another tenant's assets, tenant unit arms room in an installation-owned facility, or the storage of hazardous material in an installation-owned facility.

(1) When an Army organization exposes another Service's or another nation's personnel to a hazard the risk acceptance authority must communicate that risk to the exposed personnel's chain of command at a level equivalent to the risk acceptance authority.

(2) For all hazards that expose the public to high or extremely high risk, the risk acceptance authority will be the Army headquarters commanding general.

Table 4–1.
Risk acceptance authority for safety standards deviation

Risk acceptance matrix[2, 3, 4, 5]				
	Duration of risk			
	Event waiver	**Waiver**		**Exemption**
Category of risk	1 month or less	1 month to 1 year	1 year to 5 years	Permanent or greater than 5 years
Extremely high risk	General officer (GO)	Army Headquarters Commanding General (CG)	Army Headquarters CG	Army Headquarters CG
High risk	Brigade commanding officer (CO) or responsible O–6	GO	GO	GO
Medium risk	Battalion CO[1] or responsible O–5	Brigade CO[1] or responsible O–6	GO[1]	GO[1]
Low risk	Company CO or responsible O–3	Battalion CO[1] or responsible O–5	Brigade CO[1] or responsible O–6	Brigade CO[1] or responsible O–6

Legend for Table 4-1.:

In organizations led by Army civilian leaders, equivalent civilian grades may be substituted for military ranks (see table 4–2).

The term "Army Headquarters CG" used in the table refers to Army commands (ACOMs), Army service component command (ASCCs) (including Joint Forces Land Component Commands (JFLCC) and GO level Joint Task Forces (JTFs)), direct reporting units (DRUs), and the Director, Army National Guard.

Notes:

[1] May delegate in writing authority to accept at the next lower command level.

[2] For deviations involving violations of AE or chemical agent safety standards during Joint operations planning, training, and execution, refer to CJCSI 4360.01 and Service risk acceptance guidance. See also paragraph 4–6*i*.

[3] H risk (beyond 1 month) or EH risk will always be accepted by a GO or flag officer.

[4] For hazards discovered in fielded acquisition programs, risk will be accepted per DA Pam 385–16.

[5] Deviations from range standards and procedures are addressed in AR 385–63.

Table 4–2.
Military–Army civilian equivalent grades

Military rank	O–7 though O–10	O–6	O–5	O–4	O–3
Army civilian grade	Senior executive service (SES)–1 through SES–6	General schedule (GS)–15 or equivalent	GS–13 and GS–14 or equivalent	GS–12 or equivalent	GS–10 and GS–11 or equivalent

4–5. Deviation documentation and risk acceptance

a. When intentionally deviating from written safety standards, documentation will include specifics regarding the initial and residual levels of risk associated with the deviation, the policy and/or standard (that is, the publication and paragraph numbers) from which the operation will deviate, the control measures selected, and the required level of risk acceptance per table 4–1. Safety offices need to track and review all approved deviations for trends. Deviations (waivers, exemptions, and secretarial certifications) involving AE or chemical agents must be documented using DA Form 7632. DA Form 7632 may also be used to document safety deviations other than those involving AE and chemical agents.

b. Addressing a general risk, that is, a situation involving management of a risk that does not involve a standard, is referred to as risk acceptance. Risk acceptance documentation must include specifics regarding the initial and residual levels of risk, the control measures selected, and the required level of risk acceptance per table 4–1. Safety offices track and review all approved risk acceptances for trends.

4–6. Use of DA Form 7632 for documenting deviations and risk acceptance involving ammunition and explosives or chemical agents

a. Appendix C contains instructions for completing DA Form 7632. The following support documentation must accompany the DA Form 7632 for AE or chemical agent deviations: map or diagrams which depict the hazard area including quantity distance (QD) arcs and/or downwind hazard areas, preferably unclassified, clearly identifying locations and/or facilities of concern; timeline, listing milestones, to eliminate the need for deviation; and other supporting documents as necessary. The DA Form 7632 may cover multiple risks, if supported by accompanying documentation describing each hazard and associated risk covered.

b. An event waiver is a written authority that permits a temporary exception for strategic or other compelling reasons when conditions or circumstances causing the waiver arise unexpectedly and there is not enough time to comply with formal waiver submission and documentation procedures. Event waivers are for one-time emergency situations, not to exceed 1 month. Event waivers are not applicable to recurring missions as defined in paragraph 4–4*d*(1). The responsible commander must approve the event waiver in writing prior to onset of operations. Copies of event waivers involving AE or chemical agent must be provided to the organization's ACOM, ASCC, and/or DRU safety office and to the U.S. Army Technical Center for Explosives Safety (USATCES) for data collection and analysis. Event waivers involving AE or chemical agent may be documented using a memorandum or other command-specific format, and will include the following information:

(1) Type and net explosive weight (NEW) QD of munitions involved.

(2) Type of exposed site (ES). If people are present, give an estimate of the number of civilians and military.

(3) Strategic or other compelling reasons for approving the exception.

(4) Distance required versus distance available and QD standard not met.

(5) Narrative explanation outlining the reason or reasons why the explosive standards could not be met and a discussion of reasonable alternatives considered and rejected.

(6) Expected duration of event waiver.

(7) Point of contact (POC) name, grade, phone, and email.

c. A waiver is a written authority that permits temporary deviation from Army safety standards for strategic or compelling operational requirements. Waivers are granted for a period not to exceed 5 years pending termination of the waiver or correction of the waived conditions. Exceptional situations may require a waiver to be reissued to allow either completion of the operation requiring the waiver or time for completion of the corrective action. In such cases, the next higher approval authority will reissue the waiver. Copies of waivers and reviews involving AE or chemical agent must be provided to the organization's ACOM, ASCC, and/or DRU safety office, and USATCES for data collection and analysis. Copies of waivers for other safety standards may be provided to the organization's ACOM, ASCC, and DRU safety office for data collection and analysis. AE deviation waivers are reviewed annually - and non-AE and chemical deviation waivers at intervals not to exceed 2 years - to ensure risk assessments are current, to ensure that all exposures, risks, and mitigating actions are identified, and to validate the need for continuance.

d. An exemption is a written authority that permits long-term noncompliance with Army safety standards for strategic or compelling operational requirements. Exemptions may be granted by law, Congressional action, or in accordance with table 4–1. Exemptions are granted for periods over 5 years, to include permanent situations. Copies of exemptions and reviews involving AE or chemical agent must be provided to the organization's ACOM, ASCC, and/or DRU safety office, and USATCES for data collection and analysis. Copies of exemptions for other safety standards may be provided to the organization's ACOM, ASCC, and DRU safety office for data collection and analysis. AE exemptions are reviewed at intervals not to exceed 5 years to ensure risk assessments are current, to ensure that all exposures, risks, and mitigating actions are identified, and to validate the need for continuance. This review includes Secretarial Certificates, if applicable.

e. A Secretarial Certification is required for all new construction involving AE and chemical agent safety regulatory deviations. A certificate is written authority, granted by the Assistant Secretary of the Army for Installations, Energy and Environment (ASA (IE&E)) to build or perform a major modification on a facility or structure in violation of the provisions of AR 385–10 dealing with AE or chemical agents, DA Pam 385–61, or DA Pam 385–64. Secretarial Certifications only require one-time approval for construction and/or modification of the facility or structure: they do not require revalidation or renewal unless there is new construction and/or modification not previously approved. However, upon completion of construction and initiation of AE or chemical agent operations, an exemption must be developed for these operations. Such exemptions are executed and reviewed in accordance with requirements in paragraph 4–6*d*.

(1) Secretarial Certifications must be approved by the ASA (IE&E) prior to expenditure of funds for the project.

(2) A package needs to be completed and submitted through the chain of command of the organization having responsibility and authority over the structure to be constructed and/or modified. The submission package includes the following information:

(a) Memorandum requesting Secretarial Certification, detailing the operational necessity or compelling reason that requires the Secretarial Certification and what alternative solutions were considered, with endorsement up the chain of command.

(b) The estimated cost and project number (if assigned).

(c) The required contents of AE or chemical safety site plans per DA Pam 385–61, DA Pam 385–64, and DA Pam 385–65.

(d) The DA Form 7632 detailing the risk associated with the deviation and acceptance by the appropriate level of command for use of the facility and/or structure per table 4–1.

(3) Requests for Secretarial Certifications are routed through the command channels most responsible for the operation or facility. The commander at each level must approve the request, accepting the risk generated by the deviation, before forwarding to the next review level. ACOM, ASCC (JFLCC/GO level JTF), and DRU commanders,

and the Director, Army National Guard are required to certify that such projects are essential due to operational necessity or other compelling reasons and must explicitly accept the risk generated by the deviation.

(4) Requests for Secretarial Certifications for construction and/or modification of an Army facility and/or structure on other Services' installations will be submitted through Army and the other Service's chain of command. The ASA (IE&E) coordinates the approved submission package with the appropriate official for the other Service.

(5) Requests for Secretarial Certifications involving off-installation exposures in foreign nations must be coordinated with the host nations in accordance with applicable international treaties and status of forces agreements prior to submission to the ASA (IE&E).

f. All DA Form 7632s must be coordinated and deconflicted with the installation master plan holder.

g. DA Form 7632s must be kept accurate and kept current. When the organization's leadership transitions, the incoming leadership must be informed of and renew the risk acceptance.

h. A DA Form 7632 or System Safety Risk Assessment should be used for chartered system development programs unless another similar document has been identified in accordance with MIL–STD–882, DA Pam 385–16, or the approved System Safety Management Plan. For Joint weapon systems, the AWSSRB will review and concur with all system safety risk assessments or equivalent documents per DA Pam 385–16.

i. Required process and procedures for deviations from AE or chemical agent safety standards that occur during Joint operations at non-enduring locations are contained in CJCSI 4360.01 (this instruction does not apply to overseas enduring or Department of Defense (DOD) installations within the United States and U.S. Territories).

(1) CJCSI 4360.01 outlines the consequence and risk identification assessment process for identifying and managing hazards and risks associated with these deviations. Army-led operations determine risk levels per chapter 3.

(2) CJCSI 4360.01 contains requirements for the acceptance of risk associated with waivers and exemptions by geographic combatant commanders and their subordinates, when delegated.

(3) CJCSI 4360.01 also outlines the process for gaining military Service Secretary approval (for example, Secretarial Certification) for military construction that cannot meet AE and/or chemical agent safety requirements.

Chapter 5
Step 4 – Implement Controls

5–1. Implementing controls

Once the commander or supervisor has identified the hazards and selected controls, the controls must be effectively implemented and documented. This involves putting selected control measures in place and undertaking those activities necessary to allow the measures to be effective. DD Form 2977 should be used to document controls and measure the effectiveness of countermeasures. Army commanders and staff must ensure controls are integrated, communicated, and understood at all levels.

5–2. Implementation steps

The most important aspect of implementing controls is clearly communicating how the controls will be put into effect, who will implement them, how they will fit into the overall operation, and how the commander expects them to be enforced.

a. Examples of ways in which controls can be implemented are—

(1) SOPs and written and verbal orders.

(2) Job requirements, job descriptions, job hazard analysis, and physical requirements.

(3) Demonstrations, rehearsals, and emergency drills.

(4) During mission, task or job-safety briefings, safety committee meetings, and back-briefs.

(5) Conducting rehearsals, walking through processes, drills, and so forth.

(6) Training on the hazards and controls.

b. Integrating new control measures in work procedures is essential. Management, supervision, and worker responsibilities may need to be clearly defined in the work procedures (see DA Pam 385–10 for additional information on SOPs).

c. The workers and others must be informed about the control measures to be implemented and the reasons for the changes. This is accomplished by providing training and instruction on the new control measures and the hazards they are protecting against. This training and instruction must, at a minimum, be provided to—

(1) All new employees.

(2) All employees given new job assignments for which training has not been previously received.

(3) All employees when the new control is first established.

(4) All employees when new substances, processes, procedures, or equipment are introduced to the workplace and present a new hazard.

(5) All employees when a new or previously unrecognized hazard is identified and controls implemented.

d. First-line supervisors are critical to implementing the controls. All supervisors have to be trained and understand the safety and health hazards to which employees under their immediate direction and control may be exposed.

e. It is also important to coordinate with adjacent units and organizations to ensure they understand the hazards identified and the controls to be implemented, especially if they will encounter the same hazards or play a role in implementing the controls.

Chapter 6
Step 5 – Supervise and Evaluate

6–1. Supervision and evaluation

Step 5 of risk management ensures that risk controls are implemented and enforced to standard. It provides the means of validating the adequacy of the selected control measures in supporting objectives and desired outcomes. Like other steps in risk management, supervision and evaluation must occur throughout all phases of any operation or activity.

6–2. Supervision

a. Supervision ensures subordinates understand how, when, and where controls are implemented and ensures that controls are implemented, monitored, and remain in place. Supervision is paramount to ensuring that complacency, deviations from policies and/or standards, and circumventions of control measures are not allowed to threaten success. Supervision also provides Army leaders with the awareness necessary to anticipate, identify, and assess any new hazards and to develop or modify controls as circumstances unfold.

b. Controls established and implemented for a prolonged period are especially "at risk" to be ignored due to overconfidence or complacency. Supervisors should—

(1) *Focus on process*. Supervisors must hold employees accountable for accomplishing process activities that prevent injuries. Supervisors must reinforce their employees' efforts and contributions towards preventing injuries.

(2) *Educate*. Supervisors explain the principles and rationale for the controls and demonstrate how the controls work.

(3) *Promote ownership*. Allow employees to participate in the implementation of controls and procedures and take control.

(4) *Set expectations*. Supervisors can facilitate a shift from other-directed to self-directed motivation by initiating a process or action with stated expectations.

(5) *Support and reward*. Support employees following safety procedures and reward them for their efforts.

(6) *Model appropriate safety-related behavior*. Supervisors must model the behavior they expect of their employees. For instance, a supervisor should always wear the appropriate PPE for any area the supervisor is visiting. If hearing protection is required, then the supervisor should be using hearing protection, too.

(7) *Conduct spot checks and unannounced visits*. Supervisors should conduct periodic spot checks and unannounced visits to the various work areas under their direction. During the visits, the supervisor should be observing adherence to safety requirements for that area and checking to assure that controls are still in place.

(8) *Report-in periodically*. Supervisors should periodically report to their supervisors on the status of the controls and how effective they are.

c. Violations of safety standards are required to be reported and recorded as prescribed in DA Pam 385–10.

6–3. Evaluation

Risk management practitioners conduct evaluation during all phases and activities of operations, including after action reports and other assessments. DD Form 2977 provides space for capturing such information and should be maintained with the after action report for record and reference. Evaluation supports several goals, including but not limited to—

a. Determining if risk levels changed during operations.

b. Adapting to changes in the situation.

c. Monitoring effectiveness of controls.

d. Making corrections to control implementation.

e. Improving the application of risk management principles in current and future operations.

6–4. Feedback

An evaluation by itself is not enough; a feedback system - continuous process improvement - must be established to ensure that the corrective or preventive action taken was effective and that any newly discovered hazards identified during the mission and/or activity are analyzed and corrective action taken. Feedback informs all involved as to how the implementation process is working, and whether or not the controls were effective. Feedback can be in the form of

briefings, lessons learned, cross-tell reports, benchmarking, or database reports. Without this feedback loop, we lack the benefit of knowing if the previous forecasts were accurate, contained minor errors, or were completely incorrect.

Appendix A
References

Section I
Required Publications

AR 385–10
The Army Safety Program (Cited in paras 1–1, 1–5, 1–5e, 4–6e, table 3–2.)

ATP 5–19
Risk Management (Cited in paras 1–1, 1–5a, 1–5e, 3–5.)

CJCSI 4360.01
Explosives Safety and Munitions Risk Management for Joint Operations Planning, Training, and Execution (Cited in paras 1–5f, 4–6i, 4–6i(1), 4–6i(2), 4–6i(3), table 4–1.) (Available at http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm.)

DA Pam 385–64
Ammunition and Explosives Safety Standards (Cited in paras 4–6e, C–2b(6), C–3a(5), C–3a(6).)

DA Pam 385–65
Explosive and Chemical Site Plan Development and Submission (Cited in para 4–6e.)

DODI 6055.1
DOD Safety and Occupational Health (SOH) Program (Cited in para 1–1.) (Available at http://www.dtic.mil/whs/directives/.)

DODM 6055.09–M
DOD Ammunition and Explosives Safety Standards (Cited in paras C–2b(6), C–3a(5), C–3a(6).) (Available at http://www.dtic.mil/whs/directives/.)

MIL–STD–882
Department of Defense Standard Practice for System Safety (Cited in paras 1–5b, 3–7a, 4–6h.) (Available at https://assist.daps.dla.mil/quicksearch/.)

Section II
Related Publications
A related publication is a source of additional information. The user does not have to read a related reference to understand this publication.

ADP 5–0
The Operations Process

AR 25–30
The Army Publishing Program

AR 70–1
Army Acquisition Policy

AR 95–1
Flight Regulations

AR 385–63
Range Safety

DA Pam 385–10
Army Safety Program

DA Pam 385–16
System Safety Management Guide

DA Pam 385–30
Mishap Risk Management

DA Pam 385–40
Army Accident Investigation and Reporting

DA Pam 385–61
Toxic Chemical Agent Safety Standards

DA Pam 385–63
Range Safety

DODI 5000.02
Operation of the Defense Acquisition System (Available at http://www.dtic.mil/whs/directives/.)

FM 6–22
Army Leadership: Competent, Confident, and Agile

Technical Circular 3–04.11
Commander's Aircrew Training Program for Individual, Crew, and Collective Training

TRADOC Regulation 350–70
Army Learning Policy and Systems

29 CFR 1910.132
Personal Protective Equipment: General Requirements (Available at http://www.gpo.gov/fdsys/.)

Section III
Prescribed Forms
Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) Web site (http://www.apd.army.mil).

DA Form 7632
Deviation Approval and Risk Acceptance Document (DARAD) (Prescribed in para 1–8e.)

Section IV
Referenced Forms
Unless otherwise indicated, DA forms are available on the APD Web site (http://www.apd.army.mil); DD forms are available on the Office of the Secretary of Defense Web site (http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm).

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 2977
Deliberate Risk Assessment Worksheet

Appendix B
DD Form 2977 Instructions

B–1. DD Form 2977
DD Form 2977 is the Army's standard form for documenting risk assessment and approval and provides a tool for units to logically apply the five steps of risk management. It is available in both hard copy and electronic form and may be filled out electronically or free-hand. DD Form 2977 is designed to be used as a living document as changes occur, or new information is gleaned, during the mission and/or task being assessed.

B–2. Instructions for completing DD Form 2977
a. Page 1 provides areas for identifying the event or operation, preparer information, an area to capture information used in the five-step process, identification of the overall residual risk level, and approval authority information. Block

1 (Mission/Task Description) should include the date(s) of the mission, block 2 (Date) is to be completed with the date the DD Form 2977 was prepared.

b. Page 2 provides a standard risk assessment matrix, an area for review (used for on-going operations), an area to capture feedback and lessons learned, and an area for additional comments or remarks.

c. Page 3 provides basic instructions for completing each block of the form.

Appendix C
DA Form 7632 Instructions

C–1. DA Form 7632

a. DA Form 7632 is a four-page automated form for documenting risk management and acceptance. Use of this form is mandatory for deviations from AE or chemical agent safety standards.

b. Page 1 of the form contains information necessary for the approval authority to decide whether to approve the deviation and accept the associated risk, including location information, violation information, and documentation of deviation approval and risk acceptance. Page 2 is a worksheet used to document the risk assessment and should be completed before page 1.

c. When used for deviations involving AE or chemical agent, the Ammunition and Explosives Worksheet, found on pages 3 and 4 of the DA Form 7632, must be completed. This worksheet provides for documentation of information on the potential explosion site (PES), ESs, and potential consequences from AE or chemical agent incident and should be completed before page 1.

C–2. Completing the DA Form 7632

a. Site information. This section on page 1 identifies the site the DA Form 7632 covers. Dropdown menus are provided to help with standardization.

(1) Block 1a - Country. Enter the country where the site is located. The default is set to United States.

(2) Block 1b - State. Enter the state where the site is located or select not applicable for sites outside the United States and its territories.

(3) Block 2 - Service. Select the Service responsible for submitting the deviation.

(4) Block 3a - Installation Type. Enter the type of installation on which the site is located (for example, Fort, Base, Forward Operating Base). Select "other" for sites not on an installation.

(5) Block 3b - Installation Name. Enter the name of the installation, if applicable. For example, enter "Hood" if Fort Hood is the installation. There is no need to put "Fort Hood" in this block when "Fort" was entered in block 3a.

(6) Block 3c - Type of Site. Enter the type of the site on which the deviation occurs. This block should convey the nature of the operation involved (for example, hospital, dining facility, ammunition holding area, ammunition turn-in, driver training, and so forth).

b. Deviation information. This section on page 1 provides all the violation information at a glance and allows the approval authority to see all the critical information on one page. A portion of the blocks on page 1 will auto populate from page 2.

(1) Block 4 - Deviation number. This is the originator's unit identification code (UIC), the type of deviation (see block 7), followed by the 4–digit year, 2–digit month, 2–digit day (see block 10) and a sequential alpha character for each deviation of the type prepared that day. For example, for the second event waiver (EW) initiated by the activity with UIC W4QUAA on 10 April 2013, the individual preparing the DA Form 7632 would enter "W4QUAA–EW–20130410–B." (There are several methods for determining the UIC. The submitter of the originating unit can find their UIC in block 44 on SF–50 actions. Another way is by logging into Army Knowledge Online and going to "My Account." Select "Account Information" and scroll down to "Total Army Personnel Record" and locate the UIC. It is possible the analyst may not be associated with the originating unit and will need to find the unit's UIC. The analyst can go to the Web site below and submit a System Access Request to gain access to UIC search system at https://www.dmdc.osd.mil/appj/uicss/.) The Deviation number will automatically be inserted on the top of each sequential page of the DA Form 7632 to ensure continuity of the document.

(2) Block 5a - Effective Date. No data entry required. This block will auto populate from block 16a (Date) and will also be automatically inserted on the top of each sequential page.

(3) Block 5b - Expiration Date. No data entry required. This block will auto populate from block 16b (Expiration Date) and will auto populate the Expiration Date block on the top of each sequential page.

(4) Block 6 - Deviation From. Choose the appropriate type of standards from the dropdown list. Enter the type of standard from which the activity will deviate.

(5) Block 7 - Type of Deviation. Enter whether the deviation is an EW, waiver (W), exemption (E), or Secretarial Certification.

(6) Block 8a - Number/Title and Paragraph of Requirement. Enter the title, number, and paragraph of the requirement not being met. For example, Ammunition and Explosives Safety Standards, DA Pam 385–64, paragraph 17–2f(2). When the deviation involves a violation of Department of Defense Manual (DODM) 6055.09–M, include the appropriate reference for that document as well (for instance, DOD Ammunition and Explosives Safety Standards, DODM 6055.09–M–V1, paragraph V1.E8.2.1).

(7) Block 8b - What we need to do that deviates from block 8a. Provide a synopsis of the risk being taken. This is a synopsis of block 24.

(8) Block 8c - Operational, Strategic or Compelling Reason for Deviation. Explain the operational, strategic, or compelling reason to justify violating the safety standards identified in block 8a.

(9) Block 9 - Potential Consequences of Deviation from Approved Standards. These numbers quantify the potential consequences of the risk being accepted and are based on the residual risk after control measures on page 2 have been implemented. Enter the anticipated numbers for fatalities, additional injuries, and the dollar loss to equipment and facilities due to the deviation, based on the worst case scenario.

(10) Block 10 - Date Deviation Initiated. Enter the date the safety professional and/or analyst created this DA Form 7632.

(11) Block 11 - Residual Severity. Identify the residual severity after controls identified on page 2 have been implemented.

(12) Block 12 - Residual Probability. Identify the residual probability after controls identified on page 2 have been implemented.

(13) Block 13 - Residual Level of Risk. No data entry required. The residual level of risk will be automatically calculated based on the severity and probability entered in blocks 11 and 12.

(14) Block 14a - Safety Professional/Analyst. Enter the name and POC information of the safety professional and/or analyst that conducted the risk assessment. This will allow the "Reviewed By" official to contact the safety professional and/or analyst if questions arise.

(15) Block 14b - Analyst Signature. Signature of the safety professional and/or analyst that conducted the risk assessment. Do not sign until the risk analysis has been completed.

(16) Block 14c - Submitter's Signature. Enter the name and POC information, if different than block 14a.

(17) Block 14d - POC Signature. Signature of the submitter, if different than block

(18) Block 14e - Reviewed By. This section lists offices that have reviewed the risk assessment and have concurred or non-concurred. Routing for the DA Form 7632 should not be assumed to be through the garrison commander only. Routing for approval and proper awareness should include the garrison commander (for coordination with safety, master planning, Department of Public Works, security, fire and emergency services, environmental, legal, and so forth), senior commander (overall responsible for the installation), the higher headquarters of the unit responsible for the mission or operation, and any exposed units (to include other Services and/or agencies and non-DOD entities). See example in figure D–2. Enter the date, whether they concur with approving the deviation and accepting the associated risk, organization, printed name and title of the person reviewing, and their signature. Comments should be attached, as necessary, and the safety professional and/or analyst should consider changing the original risk assessment, if necessary, based on these comments. If a reviewer does not concur, they must select the attachment block to provide comments for their non-concurrence. If additional space is needed to document DA Form 7632 routing, create and attach additional (separate) page 1 documents. These "continuation pages" will have blocks 1 through 4 completed and "CONTINUATION OF BLOCK 14e" entered in block 8a.

c. Deviation Approval/Risk Acceptance. The section on page 1 identifies the person approving the deviation and accepting the associated risk. The person signing must be authorized to accept the risk in accordance with table 4–1.

(1) Block 15a - Army HQ. From the dropdown select the Army Headquarters (HQ) - Headquarters, Department of the Army (HQDA), ACOM, ASCC or DRU (or COCOM for combatant command, if appropriate) - the acceptance authority falls under.

(2) Block 15b - Unit/Comm. Enter the specific unit and/or command the approval authority is assigned.

(3) Block 16a - Date. Date the approving authority signs the document accepting the risk. This date will automatically populate the "Effective" date in block 5a and the top of each sequential page.

(4) Block 16b - Expiration Date. To be completed by approval authority. Enter the date the deviation will expire. The expiration date is calculated by using block 16a and the duration chosen from blocks 21a through 21d. This date should be consistent with the "Duration of Deviation" selected in either block 21a, 21b, 21c, or 21d. The Expiration Date will auto populate block 5b and the top of each sequential page once block 16b has been populated. For example, for effective date 20131202 (block 16a) and duration of 1 month to 1 year (block 21b), 12 was selected from the dropdown. The expiration date would be 12 months from the effective date. The deviation would expire on 20141201. If the deviation is greater than 5 years enter "permanent" in the space provided for the expiration date.

(5) Block 17 - Rank/Title. Rank and title of the approving authority. For example, Major General, USA, 4th Infantry Division, Commanding.

(6) Block 17a - Printed Name. Printed name of the approving authority.

(7) Block 17b - Signature. Signature of the approving authority. Electronic signature capability is provided.

(8) Block 17c - Comment. Comments should be attached, as necessary. If an approving authority comments and/or does not accept the assessed residual risk, then those developing the risk assessment should work together with the approving authority to mitigate and manage the risk to meet mission requirements. If more room is needed for comments, attach a continuation sheet and check the "attachment" block to indicate that something is attached.

d. Risk Assessment Worksheet – page 2. The Deviation number is an installation specific number for tracking purposes and will auto populate from block 4. The effective and expiration dates (block 5a) will auto populate from blocks 16a and 16b.

(1) Block 18 - Current Situation. Provide a description of the situation that necessitates this deviation. For example, briefly describe the status of the planned operation, the ongoing activity that is unsustainable and needs to change, and/or the current deviation, as applicable. Use a continuation sheet, if necessary, and check the "attachment" block indicating that something is attached.

(2) Block 19 - Hazard Category. From the dropdown, enter the broad category of the hazard that is being created by the deviation (for example, fire, weather, explosion).

(3) Block 20 - Specific Hazard. Enter a brief description of the specific hazard being created by deviating from requirements (for example, fire due to linking extension cords).

(4) Block 21 - Duration of Deviation. Choose one block to document the period of the deviation and, with the exception of block 21d, select a duration from the dropdown menu in the appropriate block (for example, block 21a, 21b, or 21c). If the deviation is permanent or greater than 5 years, enter "permanent" in the space provided or the specific number of years, if known. The expiration date (block 16b) will be calculated by the effective date (block 16a) and the specific duration entered in block 21a, 21b, 21c, or 21d.

(5) Block 22 - Deviation Approval Authority (or equivalent). Select the appropriate approval authority level in accordance with table 4–2. Military positions are listed in the drop down with the Army civilian equivalent. Army civilian equivalent grades per table 4–1 are authorized.

(6) Block 23 - Mission Impact of Not Accepting Risk. Describe the impact on the mission if the deviation and risk are not accepted (for example, mission must be cancelled, mission must be postponed until hazard can be corrected, or mission violates Army requirements). Use a continuation sheet, if necessary, and check the "attachment" block indicating that something is attached.

(7) Block 24 - What we need to do that deviates from block 8a. Provide a detailed description of the action that deviates from the safety standards identified in block 8a. A synopsis of this information will be provided in block 8b. If more room is needed for a detailed explanation, attach a continuation sheet and check the "attachment" block to indicate that something is attached.

(8) Block 25 - Control Measures. List the control measures that will be implemented to reduce the initial risk to a residual risk. Include milestones of when controls will be implemented if not implemented before the DA Form 7632 is signed. If more room is needed for explanation, attach a continuation sheet and check the "attachment" block to indicate that something is attached.

(9) Block 26 - Permanent Corrective Actions (with milestones). Permanent measures may or may not be possible. Provide milestones for any permanent actions that will be taken. For military construction projects, provide the project number and estimated cost. If more room is needed for explanation, attach a continuation sheet and check the "attachment" block to indicate that something is attached.

(10) Block 27 - Alternatives Considered. List the alternative solutions considered and the reason these were not used. Explain the reason, if an appropriate one is not listed in drop down box. Explain if no alternative solution is available. (For example, the host nation directed which port or berth to use.) Use a continuation sheet, if necessary, and check the "attachment" block indicating that something is attached.

(11) Block 28 - Attach any Supporting Documents. Check this block if supporting documents (other than the continuation pages from the above sections) are attached so the reviewers know to look for them (for example, photos, maps, drawing).

C–3. Additional considerations when completing the DA Form 7632 when deviations involve ammunition and explosives or chemical agents

When a deviation involves AE or chemical agent, complete the Risk Assessment Worksheet (page 2) and the Ammunition and Explosives Worksheet (page 3) of DA Form 7632 before completing page 1. Block 9 - Potential Consequences of Deviation from Approved Standards (block 9a (Fatalities), block 9b (Injuries), and block 9c (Equip/Fac Loss) will auto populate once blocks 39a through 39c have been populated if AE is the source of the risk. The Ammunition and Explosives Worksheet is required when a deviation involves AE or chemical agent. Information needed to populate this worksheet can be found at various organizations, but not limited to: the safety office, Department of Public Works (DPW), master planner, fire department, Director of Logistics, security and/or Military Police, property book office, and so forth. For technical assistance with this worksheet, contact the U.S. Army Technical Center for Explosives Safety, 1 C Tree Road, Building 35, McAlester, OK 74501 at DSN: 956–8737, Commercial: 918–420–8737 or at usarmy.mcalester.usamc.list.dac-es-personnel@mail.mil or via Ammo Help located

under the "DAC" tab at https://mhp.redstone.army.mil/MhpMain.aspx.

Note. The deviation number, effective, and expiration dates will auto populate onto this page after completion of page 1 of the DA Form 7632.

a. Information on the potential explosion site.

(1) Block 29a - PES Name. Enter name of the PES (for example, Ammunition Supply Point #1, Joint Explosive Ordnance Disposal Rapid Response Vehicle Parking).

(2) Block 29b - PES Function. Describe the function of the PES (for example, unit storage, explosives loaded vehicle parking area).

(3) Block 30 - PES Number People. Enter the number of people directly related to the PES.

(4) Block 31 - PES Equip/Fac (value). Enter the sum value of the equipment and facilities at the PES.

(5) Block 32 - Required Blast Distance. Enter the calculated blast distance based upon the NEW for the most hazardous hazard division and mixing rules. (See DA Pam 385–64 and DODM 6055.09–M.) The amount of NEW is the highest expected during the requested timeframe.

(6) Block 33 - Required Fragment Distance. Enter the calculated fragment distance based upon the NEW for the most hazardous hazard division and mixing rules. (See DA Pam 385–64 and DODM 6055.09–M.)

(7) Block 34a-f - Hazard Division. Enter the NEW by hazard division.

(8) Block 35a - QD arcs exceed the installation boundary? Are other Services affected? Was coordination made? Provide other coordination documentation, as necessary. Why coordination was not made. Coordination paperwork attached? Check yes or no to indicate whether the arcs exceed the installation boundary, affect other Services, or if other coordination documents are available. State why coordination was or was not made. Check the "attachment" block to indicate that something is attached, if needed.

(9) Block 35b - Is this deviation associated with a hybrid or risk-based safety submission? Indicate yes or no if deviation is associated with an approved explosives safety site submission. The DA Form 7632 will be included in the explosives safety site submission as a supporting document.

(10) Block 35c - If yes, provide site plan number. Provide site plan number, as necessary. This is an installation specific number for their tracking purposes. For example, MCAAP–SP–2013–01. MCAAP is McAlester Army Ammunition Plant, SP indicates site plan, 2013 is the year, and 01 is the sequence number of site plans that installation has for that year or an alpha and numeric format similar to block 4 above.

b. Information on exposed sites. This section lists ESs to the PES and provides estimates of expected loss in the event of an accident. Block 36 – Exposed Sites. List the ES facility number and description of all facilities within inhabited building distance (IBD) of the PES. Enter the required and actual distances between the PES and ES. Next, enter the number of people at the ES and calculate the estimated dollar value of the ES facility and/or equipment at the ES. Then, enter the type of exposure (that is, quantity distance) relationship required between the PES and ES (for example, IBD, Public Traffic Route distance, and so forth). Next, annotate whether the ES is on or off the installation. Then, calculate the expected number of fatalities, injuries, and loss to equipment and facilities for the ES. Calculation of expected loss can be determined by using software, such as the Department of Defense Explosives Safety Board approved software Automated Safety Assessment Protocol–Explosives (ASAP–X) tool. The expected number of fatalities, injuries, and loss to equipment and facilities must be calculated twice: for each ES at the required distance and again for each ES as sited. The information entered in block 36 will be broken down in different categories in the following Expected Potential Consequences section. The violation yes/no block will auto populate based on the required and/or actual feet listed in the Distance Required and/or Actual Column. If the actual distance is greater than the required distance there will be "no" violation. The Violation Column can be manually changed, if needed. Repeat this procedure for each ES. Use a continuation sheet, if necessary, and check the "attachment" block indicating that something is attached.

c. Expected potential consequences. This section uses information from block 36 to calculate potential consequences. The different types of consequences have been calculated to reflect the impact of an incident assuming total loss of the people, equipment, and facilities at the PES.

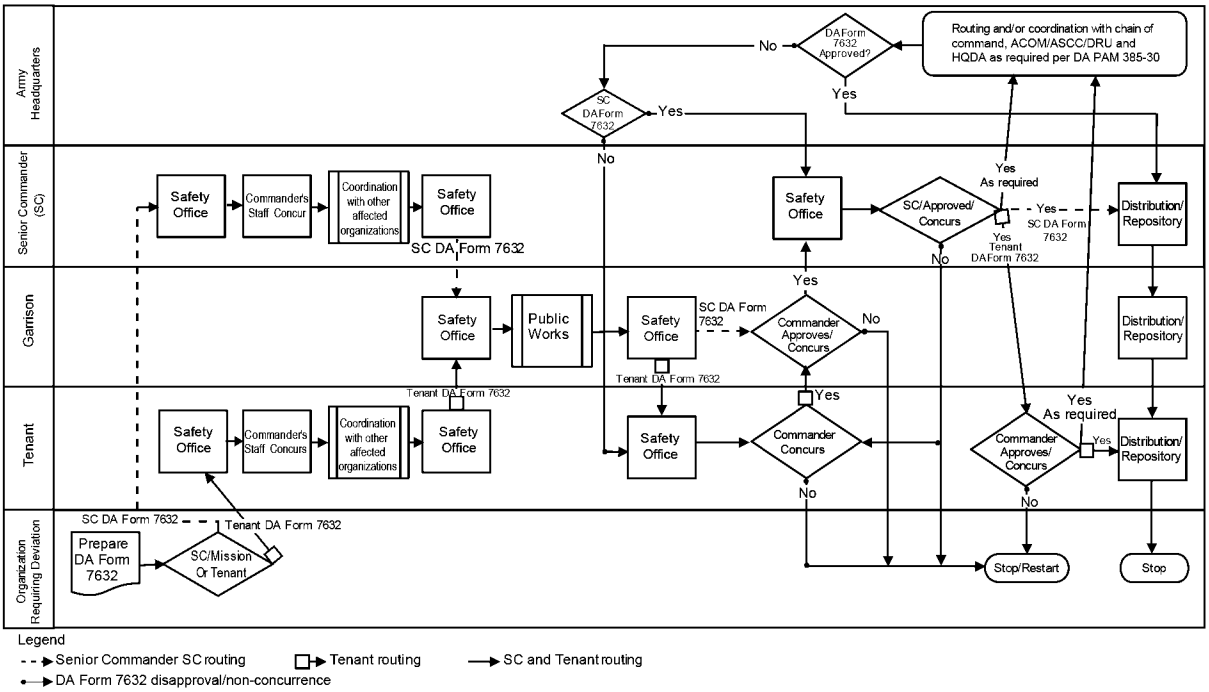
(1) Blocks 37a through c - Potential Explosion Site (PES). These numbers reflect the fatalities, injuries, and dollar loss of equipment and facilities at the PES. These numbers will auto populate and will match (assuming 100 percent loss) those entered in blocks 30 and 31. The default can be manually overridden if that is not the reality of the situation due to protective construction, testing, and so forth. For example, there could be three fatalities and two injuries associated with the PES due to protective construction versus five fatalities (100 percent loss).

(2) Blocks 38a through c - Potential Losses for Exposed Sites (ES) Meeting Criteria. These numbers reflect the potential loss for all ESs listed assuming that all meet the required distance. The values for all ESs listed that have "No" violation in Block 36 are to be summed and manually entered in blocks 38a through c based on the "at required distance" fields from block 36. These blocks may require manual input to include the totals from any continuation sheet attachments if additional space for block 36 was needed.

(3) Blocks 39a through c - Potential Loss Being Accepted for Deviating from Approved Standards. These numbers reflect the increased potential loss for ESs that are in violation of the required distance but do not include losses

entered in block 38. These fields represent the additional consequences associated with the PES and the violations being accepted. These numbers come from the difference in the "as sited" and the "at required distance" fields of block 36 for ES sites listed that have the answer "Yes" violation in block 36. Blocks 39a through c should include the totals from any continuation sheet attachments, if additional space for block 36 was needed. These blocks require manual input and will auto populate blocks 9a through c.

(4) Blocks 40a through c - Total Potential Loss. These numbers will auto populate by summing blocks 37a through c, 38a through c, and 39a through c and reflect the total potential loss if an incident were to occur at the PES.



Notes:

[1] Risk acceptance, per table 4–1, may occur at various stages of this process, depending on the risk level.

[2] The SC lane and the term "SC DA Form 7632" encompass DA Forms 7632 initiated by any local activity falling under the SC's command, including both garrison and mission organizations.

[3] The "Safety Office" in the SC lane refers to the SC's designated safety office.

Figure C–1. Example of DA Form 7632 routing

Appendix D
Application of Risk Management to Army Learning Policy and Systems

D–1. Army Learning Policy and Systems

The instructional system design process used for developing Army learning products is analysis, design, development, implementation, and evaluation (ADDIE). This spiral approach is used as the basis for the entire Army Learning Policy and Systems. The purpose of the Army Learning Policy and Systems is to support the Army by regulating practices in effective learning management and specifying required enabling systems. The requirements of the Army Learning Policy and Systems program are discussed in detail within the United States Training and Doctrine Command (TRADOC) Regulation 350–70 and its associated TRADOC pamphlets. TRADOC is the Army's proponent for structured training. Such policies and systems apply to all Army organizations (TRADOC and non-TRADOC alike) that produce, implement, and/or evaluate learning and learning systems. The major concern of all commanders is to ensure their Soldiers, Army civilians, and units are trained to perform their mission to standard and survive. To ensure mission-focused training, Soldiers, Army civilians, staff, and units must perform under realistic conditions. Risk management balances benefits against potential losses during this training. It provides commanders and leaders with the tools to accomplish realistic training and education while preserving the scarce resources of personnel, time, and

equipment. When used properly, risk management is a training and education enabler. In this chapter we will present risk management application into the Army Learning Policy and Systems.

D–2. Learning product requirements

In developing learning products, institutions must—

a. Extend learning beyond the schoolhouse in a career-long learning continuum through the use of current and emerging network technologies.

b. Design learning to be more facilitated, team-based, and learner-centric.

c. Leverage technology to provide engaging, relevant, and rigorous resident, distributed, and mobile learning, and social learning activities.

d. Leverage opportunities to implement technologies to engage and appeal to digital learners.

e. Institutionalize a progressive and sequential learning process throughout a Soldier or Army civilian's career to develop a deepening of cognitive, interpersonal, and problem-framing and/or solving skills essential for personal adaptability.

f. Design the learning system to expand beyond the confines of "brick and mortar" to deliver learning products to Soldiers or Army civilians at the point of need.

g. Implement blended learning to balance quality face-to-face learning experiences with technology-enabled learning products.

h. Employ learning strategies that foster problem-solving skills needed to enhance adaptability.

i. Continuously evaluate the entry phase characteristics and perspectives of incoming Soldiers and Army civilians and adjust learning curricula to achieve desired outcomes at all levels of the learning system.

j. Incorporate deliberate strategies to ensure required skill levels, knowledge, and abilities transfer from the institutional environment to the operational environment.

D–3. Army Learning Policy and Systems focus

The Army Learning Policy and Systems uses ADDIE as a systematic, spiral approach to develop learning programs used to making collective, individual, and self-development training and education decisions for the Army. The Army Learning Policy and Systems determines—

a. Whether or not training or education is needed.

b. What is to be trained.

c. Who gets the training or education.

d. How well and where the training or education is presented.

e. The training and education support and resources required to produce, distribute, implement, and evaluate those products.

D–4. Training Development Capability

All developers must use the Combined Arms Command approved automated development system throughout the developmental process. The current Training Development Capability system is part of the required resourcing processes, allows for the revision of related information as changes occurs, and provides a means of sharing information to reduce redundancy. This system is currently Web-based and allows training and education developers the flexibility needed to rapidly gather expertise, integrate current doctrine into their training products, and staff products for approval in an efficient digital format. The underlying process of Training Development Capability is the five-step ADDIE process and requires a great deal of communication and coordination. Figure D–1 is a graphic representation of five-step process integration.

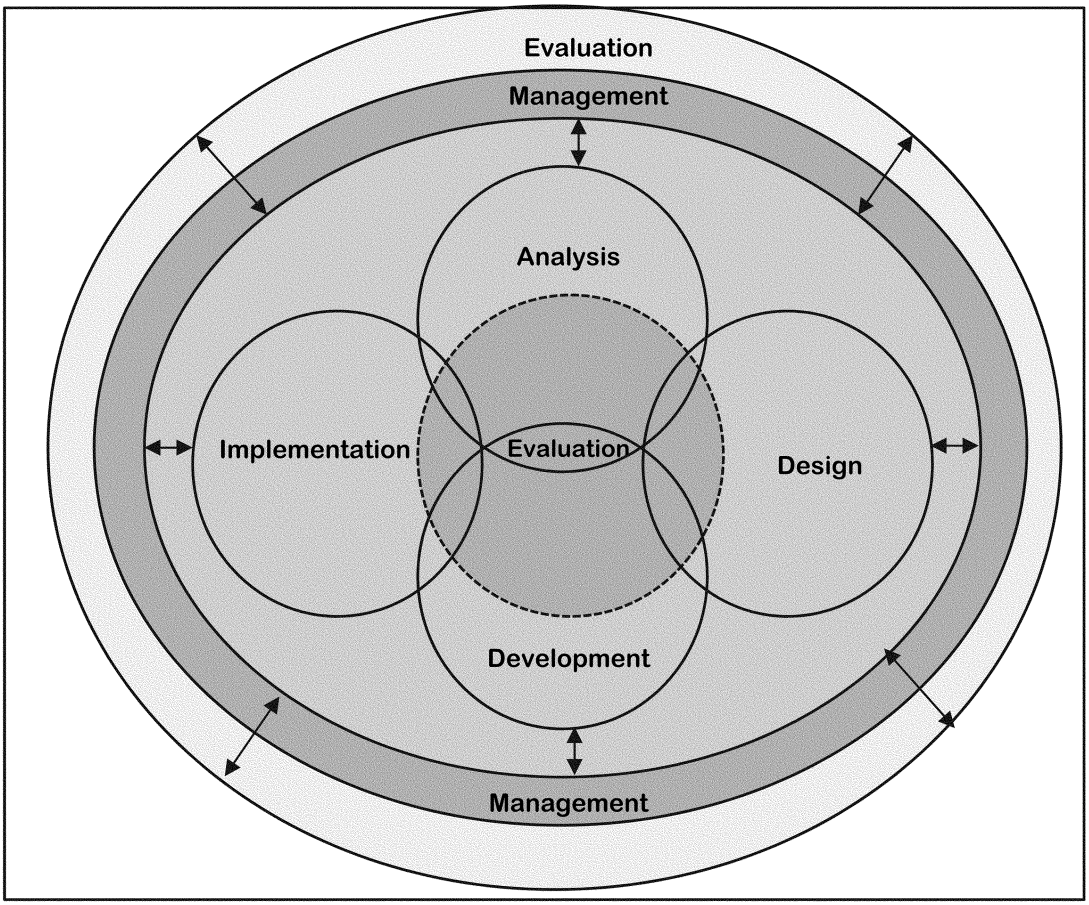
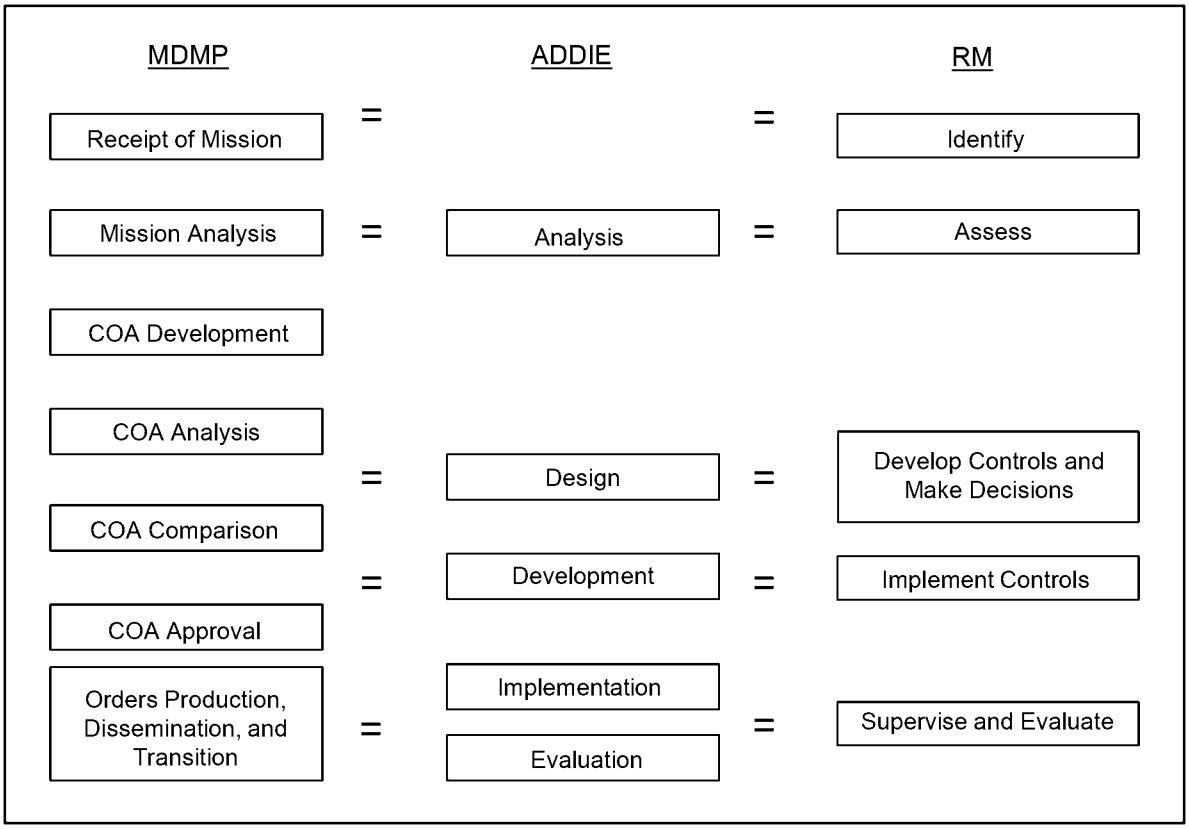


Figure D–1. The analysis, design, development, implementation, and evaluation process

D–5. Evaluation

Just as with the risk management process, evaluation is continuous throughout the ADDIE process. Feedback for corrective actions is critical. Evaluation permeates all phases. It is the cement that ensures training, education, and the required training products are effective in producing trained units and individuals. Products are evaluated either formally (product validation) or informally to determine currency, efficiency, and effectiveness. The entire process must operate within a given set of resources. The risk management process runs simultaneously and continuously to ensure training and education remains within the specified level of risk allowed for each event. The evaluation of risk management actions and the overall efficiency and effectiveness of the training are intertwined and risk management must be addressed as a part of the ADDIE process, as a whole. Figure D–2 shows the relationship between the military decisionmaking process, ADDIE, and risk management. While this graphic is not a perfect representation of the alignment, it provides a general diagram of the concepts and association of the three commonly used processes.



Legend for Figure D–2;
MDMP — military decisionmaking process
RM — risk management

Figure D–2. Analysis, design, development, implementation, and evaluation, the military decisionmaking process, and risk management

D–6. Risk management integration into training and education

a. Commanders and leaders are required to make informed risk decisions. This ensures that training and education is conducted realistically and in a manner that protects the well-being of the Soldiers and Army civilians being trained. This enables individuals, leaders, and units to recognize and mitigate hazards to improve survivability and to win over the full range of military operations.

b. Training and education developers and trainers provide safe training and education to achieve force protection by designing, developing, and implementing realistic, viable training and education that—

(1) Does not unnecessarily jeopardize lives and equipment.

(2) Eliminates or minimizes the risks involved in relation to the training and education benefits.

(3) Includes controls to eliminate or reduce the risk or hazard.

(4) Conserves and preserves resources.

(5) Complies with Federal, state, and local laws, regulations, and restrictions.

(6) Integrates safety, risk management, and force protection considerations into training, education, and training materials where appropriate.

c. Proponent training and education developers should ensure all products—

(1) Include appropriate safety, risk, and protection statements, cautions, notes, and warnings.

(2) Identify training or education risk and assign a risk level to every proponent lesson.

(3) Are staffed through the appropriate safety office director, manager, or resident safety professional for subject matter review in accordance with command guidance.

(4) Include controls necessary to minimize or eliminate hazards during training or education to include a maximum instructor to student ratio, as well as risk management procedures to be followed if the maximum ratio is exceeded.

(5) Address risk management and the risk management process as it applies operationally to the training or education subject.

d. The training development process fixes responsibility, institutionalizes operational safety, and leads to decision-making at the command level appropriate to the identified level of risk. Using risk management in the training-development process ensures the following:

(1) Safe training or education.

(2) Fewer injuries and deaths.

(3) Reduced incidents of lost time.

(4) Lower costs (facility, training, and equipment repairs).

e. Risk management is never complete. It is a continuous cycle that requires everyone be constantly alert to training risks and to take immediate action to eliminate them or reduce their severity. Safety, risk management, and accident prevention are commander's, manager's, and individual's responsibilities. Proponent training and education developers, trainers, educators, and subordinate personnel should use the generic risk management information contained in training support products to begin their review of and update to hazards, as well as the controls to adjust for current conditions. Trainers and educators need to make corrections to their risk management worksheet and processes as they relate to their subject training. Trainers and educators rely on the quality products of developers. The developers rely on feedback from the trainers, educators, safety professionals, and other subject matter expert input. The Soldier or Army civilian receiving the training or education relies on the entire team to provide quality training or education.

Appendix E
Application of Risk Management to Other Areas

The death of a Soldier in combat or due to an accident can have a devastating effect on a unit's morale and effectiveness. The effects of criminal acts, suicide, sexual assault, domestic violence, substance abuse, child abuse, and other high risk reckless behaviors can also cripple an organization's morale and destroy its combat effectiveness. Commanders and leaders must establish and maintain a command environment that fosters cohesion, team work, and performance to standard while caring for the well-being of the individual. Previous chapters discussed the application of risk management in tactical and non-tactical situations, in the training development process, and as a life skill for individual activities. Commanders and leaders can also use the risk management process to identify behaviors or activities that may present hazards to a unit's morale and impact combat effectiveness. This chapter provides examples on how risk management will be applied to mitigate a number of these hazards in some of the appropriate areas.

E–1. Leadership

a. Command issues. The principles of risk management become indispensable in addressing issues that impact Soldiers and Army civilians both on and off the battlefield. Effective risk management is on-going and cyclic. The risk management process is integrated into the development of all SOPs and the development process for all policies that address issues of behavior, health, and criminal activity. The following paragraphs discuss risk management application in the areas of sexual assault prevention, suicide prevention, and PMV accident prevention.

b. Command emphasis.

(1) By applying the principles of risk management when identifying hazards associated with suicide, sexual assault, and PMV accident prevention, commanders can take the initiative to identify and mitigate risks associated with these hazardous behaviors and situations before they impact on our units. This in no way implies these are the only applications for risk management. This five-step process can be applied across the full spectrum of human activity to identify hazards, assess risk, and make decisions.

(2) The principles of risk management as a decisionmaking tool are universal in application. The repeated use of the systematic risk management process reinforces application of the five steps to identify, assess, and control hazards and to make informed risk decisions in any situation. The risk management process is integrated into the development of SOPs as well as the development of policies that address issues of behavior, health, and criminal activity.

E–2. Sexual harassment and assault prevention

a. The prevention of sexual harassment and assault is both a command and an individual responsibility. Sexual assault destroys teamwork, undermines the good order and discipline of the military, destroys unit morale, and impacts personal combat readiness. Effective risk management identifies the potential hazards, conditions, or situations that may lead to this behavior. Early identification of conditions conducive to such behavior and active intervention by leadership reduces the likelihood of individuals attempting sexual assault or becoming a victim of a sexual assault. The principles of risk management can play a pivotal role by assisting the commander with tools to enhance policy awareness and training. By conducting command climate assessments, complaints processing awareness briefings, and overall assistance concerning the prevention of sexual harassment, commanders can mitigate the risks associated with sexual harassment and assault. Individuals must be educated on how best to avoid being a sexual assault victim. Once

armed with this knowledge and ability, individuals can avoid situations that may put them in danger or may lead to their harassment or assault.

b. The three tiers of self-protection include being alert, prepared, and assertive. See figure E–1 for a graphic representation of these protection methods. Trust your instincts; if a place or person feels unsafe, it probably is. Watch for signs of trouble such as strangers in private areas or persons loitering in places where they shouldn't be. Utilize real time risk management in order to assess the risks, develop controls, and implement those controls in order to mitigate the risks. If you sense trouble and have very little time, it may be best to get to a safe place as soon as possible. If you feel you are in danger, attract help any way you can. Implementing controls is key. Taking steps such as traveling with a buddy, staying in groups, staying sober, educating yourself about date rape drugs, walking only in lighted areas after dark, and keeping the doors to homes, barracks, and cars locked are all good ideas. However, the best control measures are useless unless they are implemented.

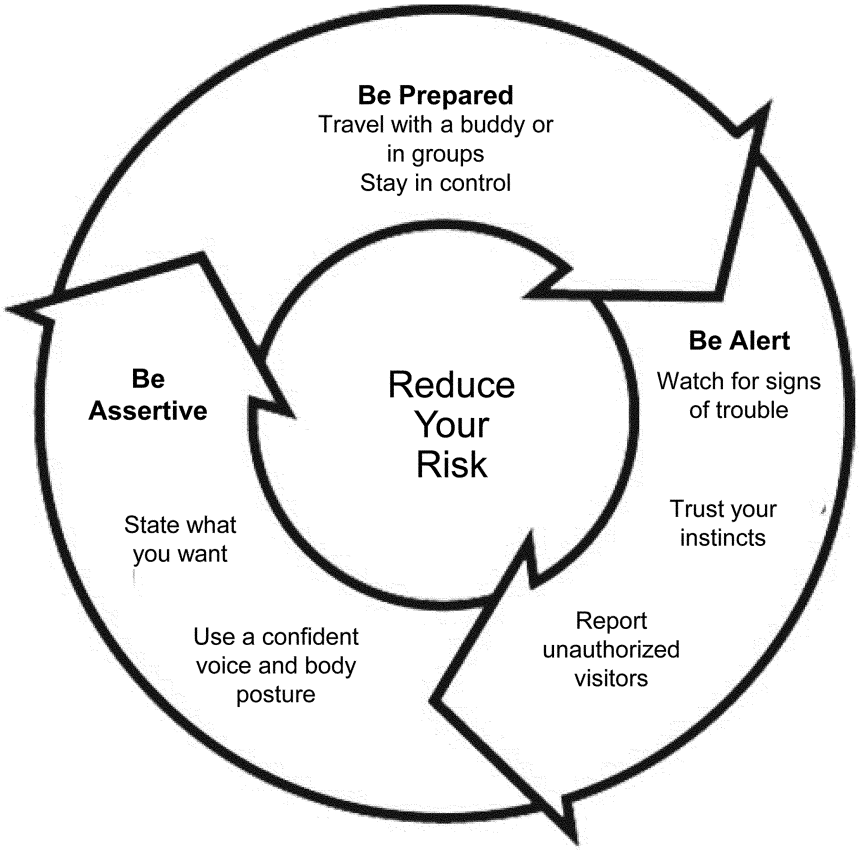


Figure E–1. Sexual assault risk reduction

E–3. Suicide prevention

a. Each year the Army needlessly loses Soldiers and Army civilians to suicide. Suicides occur across every segment of the force. Suicide prevention, like all leadership challenges, is a commander's program and there is leader responsibility at all levels. Suicide is a highly complex human tragedy. There is no typical profile of deaths by suicide. Suicide poses a significant challenge to the readiness of our force. The principles of risk management and the five-step process are relevant and critical in identifying, assessing, and mitigating suicide risk to personnel. The role of Army leadership in suicide prevention cannot be overemphasized. Leaders, as well as fellow Soldiers, Army civilians, and Family members are the first line of defense to recognize personnel who are experiencing life stressors. They can take

appropriate actions to prevent further loss of life and utilize numerous support resources to assist personnel in lowering their risk level. It is important for all commanders and leaders to recognize that mental wellness is a key component for overall individual readiness and fitness.

b. Commanders and leaders should make use of tools that provide a comprehensive, continuous, and standardized process to assess the well-being of their Soldiers and Army civilians, ensure intervention strategies are in place to assist those individuals, and significantly reduce high risk behaviors. Tools provided by the Army and major commands to assist commanders include:

(1) The Army Readiness Assessment Program (ARAP). ARAP is a tool that addresses root causes of accidental loss by focusing on organizational safety climate and culture. ARAP is an online assessment, filled out by employees and Soldiers anonymously, that captures unit posture on command and control, standards of performance, accountability, and risk management. ARAP provides battalion-level commanders with data on their formation's readiness posture.

(2) The United States Army Soldier Leader Risk Reduction Tool may be found at www.preventsuicide.army.mil. This tool may be used in conjunction with appendix B of Field Manual (FM) 6–22 to counsel individuals. These tools should be used during developmental counseling sessions. Additional information on suicide prevention training, current guidance, and an expanded commander's toolbox may also be found at this site. Civilian employees may contact their Occupational Health Clinic or their local Installation Employee Assistance Office for additional information.

E–4. Private motor vehicle accident prevention

PMV accidents have historically been the leading cause of accidental death for Soldiers. Every Soldier has an individual responsibility to prevent accidents. Commanders and leaders must also be vigilant in the identification of high-risk behavior. Risk management assists commanders and leaders in recognizing those hazards, behaviors, and/or situations that may lead to tragedy. The Director of Army Safety has prepared a number of tools to help leaders manage PMV risk.

a. The Travel Risk Planning System (TRiPS) is an automated trip planning tool that incorporates the principles of Risk Management and facilitates a dialogue between supervisor and subordinate prior to privately owned vehicle travel.

b. These tools are available through the U.S. Army Combat Readiness/Safety Center at https://safety.army.mil.

Glossary

Section I
Abbreviations

ACOM
Army command

ADDIE
analysis, design, development, implementation, and evaluation

ADP
Army doctrine publication

AE
ammunition and explosives

APD
Army Publishing Directorate

AR
Army regulation

ARAP
Army Readiness Assessment Program

ASA (IE&E)
Assistant Secretary of the Army (Installations, Energy and Environment)

ASAP–X
Automated Safety Assessment Protocol-Explosives

ASCC
Army service component command

ATP
Army techniques publication

AWSSRB
Army Weapon System Safety Review Board

CFR
Code of Federal Regulations

CG
commanding general

CJCSI
Chairman of the Joint Chiefs of Staff instruction

CO
commanding officer

COA
course of action

COCOM
combatant command

DA
Department of the Army

DA Pam
Department of the Army pamphlet

DARAD
Deviation Approval and Risk Acceptance Document

DD
Department of Defense (form)

DOD
Department of Defense

DODI
Department of Defense instruction

DODM
Department of Defense manual

DPW
Department of Public Works

DRU
direct reporting unit

DSN
Defense Switched Network

E
exemption

EH
extremely high

ES
exposed site

EW
event waiver

FM
field manual

GO
general officer

GS
general schedule

H
high

HQ
headquarters

HQDA
Headquarters, Department of the Army

IBD
inhabited building distance

JFLCC
Joint Forces Land Component Commands

JTF
joint task force

L
low

M
medium

MDMP
military decisionmaking process

MIL–STD
Military standard

NEW
net explosive weight

O
officer

OPORD
operations order

OPTEMPO
operating tempo

PES
potential explosion site

PM
program manager

PMV
private motor vehicle

POC
point of contact

PPE
personal protective equipment

QD
quantity distance

RAC
risk assessment code

RM
risk management

SA
situational awareness

SC
senior commander

SES
senior executive service

SF
standard form

SOH
Safety and Occupational Health

SOP
standing operating procedure

SP
site plan

TRADOC
U.S. Army Training and Doctrine Command

TRiPS
Travel Risk Planning System

UIC
unit identification code

USATCES
U.S. Army Technical Center for Explosives Safety

W
waiver

Section II
Terms

Army Weapon System Safety Review Board
Focuses on the safety of Joint Service weapon systems. The AWSSRB represents Army in Joint weapon safety reviews; provides technical expertise to the Office of the Director of Army Safety, the Deputy Assistant Secretary of the Army (Environment, Safety and Occupational Health) and other Army Staff regarding weapon system safety related policy, standards, and technical issues; supports the DA System Safety Council in the identification and resolution of system safety issues; supports PMs; and interfaces with other Army safety review boards for Joint systems.

Asset
Something of value. Assets include but are not limited to Soldiers, personnel, facilities, equipment, operations, data, the public, the environment, equipment, and systems.

Exemption
A written authorization granted by the proper Army authority for strategic or other compelling reasons that permits a long-term deviation from mandatory Army safety requirements.

Fault
An abnormal undesirable state of a system, a system element, or process induced by the presence of an improper command (or absence of a proper one) or a failure (see definition below). All failures cause faults; not all faults are caused by failures. A system which has been shut down by safety features has not faulted.

Failure
Loss of functional ability to perform as intended (for example, relay contacts corrode and will not pass rated current closed; the relay coil has burned out and will not close the contacts when commanded—the relay has failed; a pressure vessel bursts—the vessel fails; or operator does not perform as required). A protective device that functions as intended has not failed (for example, a blown fuse).

Frequency
Rate of mishap occurrence. Frequency is sometimes substituted for probability as a component of risk (for example: loss events per 100 operating hours).

Hazard
A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation.

Hazard analysis
Refers to a number of methods for identifying process hazards, measuring their relative consequences, and deriving recommendations.

Hazard list
A simple listing of hazards that may exist in the activity under evaluation. The possible hazards are listed by possible source without regard for the mechanism, outcome, or any consideration of likelihood of being present.

Hazard matrix
An analysis technique where a table is developed listing potential hazards versus potential failures areas in the activity being evaluated. Examples of hazards are corrosion, fire, impact, shock, and so on. Examples of potential failure areas are mechanical, personnel, or procedural.

Hazard scenario
A postulated sequence or development of events in which the existence of a hazard has the potential for causing a mishap.

Maximum credible event
The most disastrous maximum credible loss identified for a given system or operation. In AE and chemical agent hazards evaluation, the maximum credible event due to a hypothesized accidental explosion, fire, or toxic chemical agent release (with explosives contribution) is the worst single event that is likely to occur from a given quantity and disposition of AE. The event must be realistic with a reasonable likelihood of occurrence considering the means of initiation, explosion propagation, burning rate characteristics, and physical protection given to the items involved. The maximum credible event evaluated on this basis may then be used as a basis for effects calculations and casualty predictions.

Maximum credible risk
The risk associated with the hazard which is the most severe and the most credible.

Military decision making process
An interactive planning methodology to understand the situation and mission, develop COAs, and produce an operation plan or order (see ADP 5–0).

Mishap
An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Mishap probability
Likelihood of mishap occurrence over a specified exposure interval. Probability is expressed as a value between zero and one. Probability is a component of risk and has no dimension but must be attached to an interval of exposure (for example, 1 operating year, 1 million vehicle miles).

Negligence (law)
Failure to exercise the degree of care considered reasonable under the circumstances, resulting in an unintended injury to another party. Negligence uses the "reasonable person" standard. In cases involving negligence, which is an unintentional injury, the law asks whether or not a reasonable person in the position of the defendant would have anticipated and guarded against the risks inherent in his or her conduct.

Probability
In risk analysis, the likelihood that an event will occur. There are five categories (with associated codes) of probability: frequent (A), likely (B), occasional (C), seldom (D), and unlikely (E).

Residual risk
The risk associated with a hazard that remains after implementing all planned countermeasures or controls to eliminate or control the hazard. The residual risk can also be the initial risk.

Risk
Probability and severity of loss linked to hazards.

Risk assessment
The process of identifying and characterizing hazards, analyzing them for their potential mishap severity and probability (or frequency) of occurrence, and prioritizing them for risk mitigation actions. The first two steps of the risk management process.

Risk category
A specified range of risk associated with a given level (high, serious, medium, low) used to prompt specific action, such as reporting hazards to appropriate management levels for risk acceptance.

Risk control hierarchy
Prioritized ranking of methods for controlling risk, arranged by order of effectiveness: (1) elimination; (2) substitution of less hazardous materials, processes, operations, or equipment; (3) engineering controls; (4) warnings; (5) administrative controls; and (6) PPE.

Risk decision
The decision to accept or not accept the risk(s) associated with an action; made by the commander, leader, or individual responsible for performing that action and having the appropriate resources to control or eliminate the risk's associated hazard.

Risk management
The process for managing risk, continuously applied across the full spectrum of Army training and operations, individual and collective day-to-day activities and events, and base operations functions to identify and assess hazards, develop and implement controls, and evaluate outcomes. The process of identifying and providing recommendations on whether to resolve or to accept accident-producing hazards associated with a mission; the design of a system, facility, equipment, or processes; and their operation.

Secretarial Certification
A written authorization granted by the Assistant Secretary of the Army for Installations, Energy and Environment for strategic or other compelling reasons that permits long-term noncompliance with mandatory Army safety requirements.

Severity
The expected consequence of a mishap in terms of degree of injury, property damage, or other mission impairing factors (loss of combat power and so on). There are four categories (with associated codes) of severity: catastrophic (I); critical (II); moderate (III); or negligible (IV).

Tolerable risk
The level of risk associated with a specific hazard below which a hazard does not warrant any expenditure of resources to mitigate.

Troop leading procedures
A dynamic process used by small unit leaders to analyze a mission, develop a plan, and prepare for an operation (see ADP 5–0).

Unnecessary risk
A risk that can be reduced or eliminated without adversely affecting the successful accomplishment of the mission.

Waiver
A written authorization granted by the proper Army authority for strategic or other compelling reasons that permits a temporary deviation from mandatory Army safety requirements.

Section III
Special Abbreviations and Terms
This section contains no entries.