CJCSM 3105.01C
10 July 2026

JOINT RISK ANALYSIS METHODOLOGY

JOINT STAFF
WASHINGTON, D.C. 20318

(INTENTIONALLY BLANK)

CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-5 CJCSM 3105.01C
DISTRIBUTION: A, B, C 10 July 2026

JOINT RISK ANALYSIS METHODOLOGY

References:
a. CJCSI 3100.01F, 29 January 2024, "Joint Strategic Planning System"
b. CJCSM 3130.06E, 12 May 2026, "Global Force Management Allocation Policies and Procedures"
c. CJCSI 3401.02B, current as of 17 July 2014, "Force Readiness Reporting"
d. ICD 203, 12 June 2023, "Analytic Standards"
e. Title 10, U.S. Code, section 153

1. Purpose. This manual establishes the Joint Risk Analysis Methodology (JRAM) and provides guidance for appraising, managing, and communicating risk. It describes a common risk lexicon to facilitate consistency across Department of War (DoW) and Joint Force risk-related processes, and is the defining methodology for describing risk on the Joint Staff.

a. The JRAM enables the Chairman of the Joint Chiefs of Staff (CJCS) to make consistent, timely risk appraisals and provide military advice on risk management in support of title 10 responsibilities, including, but not limited to, the *National Military Strategy* (NMS) and *Chairman's Risk Assessment* (CRA). The JRAM places the CRA in the context of other Joint Force processes, illustrates how risk connects these efforts, and provides a framework for the Joint Force to use and adapt for all Joint Strategic Planning System (JSPS) risk-related processes.

b. While several Joint Staff documents address risk, this is the authoritative Joint Staff risk reference that supports the JSPS.

2. Superseded. CJCS Manual 3105.01B, 22 December 2023, "Joint Risk Analysis Methodology" is hereby superseded.

3. Applicability. The JRAM applies to the Joint Staff, Services, Combatant Commands (CCMDs), relevant defense agencies, and joint and combined activities. These organizations must apply the principles outlined in this manual across their spectrum of responsibilities.

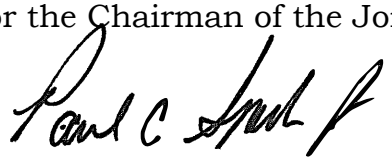
4. Procedures. See Enclosures A through C.

5. Summary of Changes. Pillars of Risk in Enclosure B have been re-organized and expanded to better describe in detail how to conduct each step of analysis. A fifth pillar, "Risk Review and Refinement," has been added. An Intelligence Community (IC) crosswalk section has been added to Enclosure C to facilitate translation of methodology between the JRAM and IC tradecraft. Call-out boxes were added to enhance risk assessments in the areas of risk-context and risk as opportunity. Quantitative risk analysis has been conceptually introduced and described. Risk of inaction, calculated risk, and opportunity cost have been defined and detailed. Military Strategic Risk (MSR) and Military Risk (MR) definitions have been adjusted to provide clarity to users, and Future Military Risk has been defined. Various figures have been added to aid in conducting temporal risk analysis, including comparative analysis and visualization of risk tradeoffs across time. Language across the JRAM has been updated to provide increased clarity and methodology employability.

6. Release. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on the Non-classified Internet Protocol Router Network. DoW components (to include the CCMDs) and other Federal agencies may obtain copies of this directive through the Internet from the CJCS directives electronic library at: <https://dod365.sharepoint-mil.us/sites/JS-Matrix-DEL/SitePages/Home.aspx>. Joint Staff activities may also obtain access via the SECRET Internet Protocol Router Network (SIPRNET) directives electronic library at <https://intelshare.intelink.sgov.gov/sites/jointstaff/sjs/imd/directives/default.aspx>. Access by SIPRNET users and distribution within the SIPRNET community is unlimited.

7. Effective Date. This MANUAL is effective upon signature.

For the Chairman of the Joint Chiefs of Staff:



PAUL C. SPEDERO, Jr., RADM, USN
Vice Director, Joint Staff

Enclosures
- A – Risk and the Joint Force
- B – Joint Risk Analysis Methodology
- C – Risk to Strategy – Strategic Assessments
- D – Risk Documents

INTENTIONALLY BLANK

CJCSM 3105.01C
10 July 2026

TABLE OF CONTENTS

LIST OF FIGURES

1

ENCLOSURE A

RISK AND THE JOINT FORCE

1. Introduction. The JRAM presents a common methodology—consistent with risk best practices—for the Joint Force to standardize and conduct comprehensive risk analysis throughout the JSPS (reference (a)). In this methodology, commanders and their staffs appraise, manage, and communicate risk using a framework consisting of five pillars: risk identification, risk analysis, risk judgment, risk management, and review and refinement. The JRAM enhances risk communication and decision-making by using the same terms and processes to communicate MSR (risk to national interests) and MR (risk to executing the NMS, including Risk-to-Mission (RM) and Risk-to-Force (RF)). The methodology described in this manual, coupled with military judgment, determines risk levels and mitigation strategies to facilitate risk-informed decisions. While this methodology is intended to be structured to provide commonality across the Joint Force, it is flexible enough to be applied to a diverse set of risk assessments.

2. Joint Strategic Planning System and Risk. Assessing risk throughout the JSPS provides the foundation for CJCS to fulfill title 10 responsibilities to provide globally integrated military recommendations.

a. Commanders and their staffs routinely consider threats and hazards that affect operations in relation to global missions and forces required for strategy execution. They must identify and articulate “risk to what” and “risk to whom” after considering risk inputs from many organizations.

b. Figure 1 displays the nested direction and missions, and their sources (left), along with the levels of associated risks (right). This framing better enables organizations to scope, detail importance, show linkages, compare, adjudicate, and properly focus mitigations for MSR and military risk in a global strategic context.

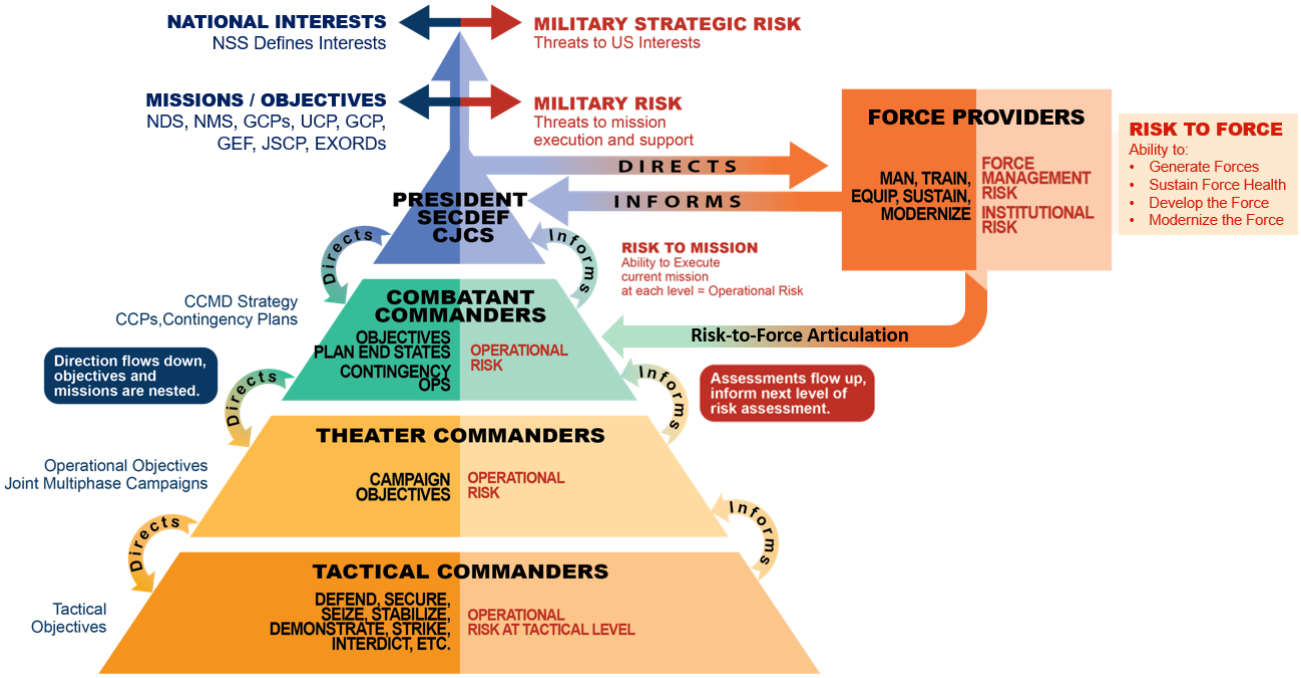


Figure 1. Organizations and Risk

3. Summary. The Joint Force works together to achieve a common understanding of globally integrated risk, accomplished primarily through JSPS processes and products. Commanders and their staffs use risk analysis to provide the best advice possible in pursuit of strategy execution. Appraising, managing, and communicating global risk lays a foundation on which to allocate resources, set priorities, and achieve national military objectives.

ENCLOSURE B

JOINT RISK ANALYSIS METHODOLOGY

1. Introduction

a. Risk is the probability (likelihood) and consequence (impact) of an event or condition causing harm to a thing that is valued. In the JRAM, the things of value are most often the objectives and interests articulated in strategic guidance. The JRAM characterizes risk across four baseline levels—*Low*, *Moderate*, *Significant*, and *High*—and may further describe them with trend modifiers that reflect expected changes over the near-, mid-, and long-term time horizons used in the JSPS. CCMDs and Services often perceive risk differently across these time horizons. CCMDs often are more operationally focused, and as such perceive risk in a more near-term fashion, whereas Services are often more institutionally focused, assessing and mitigating risk over longer periods of time.

b. Regardless of time horizon or organizational focus, the JRAM enables leaders to align their risk tolerance—the degree of risk they are willing to accept—with available options. It treats risk as arising from both action and inaction, allowing commanders and their staffs to compare the consequences of pursuing or foregoing a course of action (COA) and to weigh downside risk against potential opportunities. The methodology is primarily qualitative, drawing on quantitative analysis when appropriate. It includes recurring comparison of previous judgments against observed outcomes as part of a continuous cycle of assessment, decision, and adjustment. The JRAM's foundation rests on five constant elements: probability, consequence, time, global integration, and risk level. This framework is flexible enough for risk-related processes to adapt portions of it while maintaining these core components.

2. Framework. The JRAM framework organizes content into five pillars; however, practitioners should apply them as an integrated, continuous process: Context and Scoping → Risk Identification → Risk Analysis → Risk Judgement → Risk Management → Risk Review and Refinement. Risk Communication and Opportunity components should be applied throughout the process (Figure 2). Two additional components (Risk Appraisal and Risk Management) are discussed in Enclosure C, as they apply to the CRA and the Secretary of War's (SecWar's) related Risk Mitigation Plan (RMP).

a. Pillars

(1) Risk Identification. Identifying the threats (i.e., “risk from what?”).

(2) Risk Assessment. Developing a risk profile (i.e., “how much risk?”).

(3) Risk Judgment. Evaluating the risk (i.e., “how much risk is okay?”).

(4) Risk Management. Decisions and actions to accept, avoid, mitigate, transfer, or exploit risk (i.e., “what should we do or not do about the risk?”).

(5) Risk Review and Refinement. How well previous risk identification, assessments, judgments, and management actions performed over time (i.e., “were we effective, and how can we improve?”).

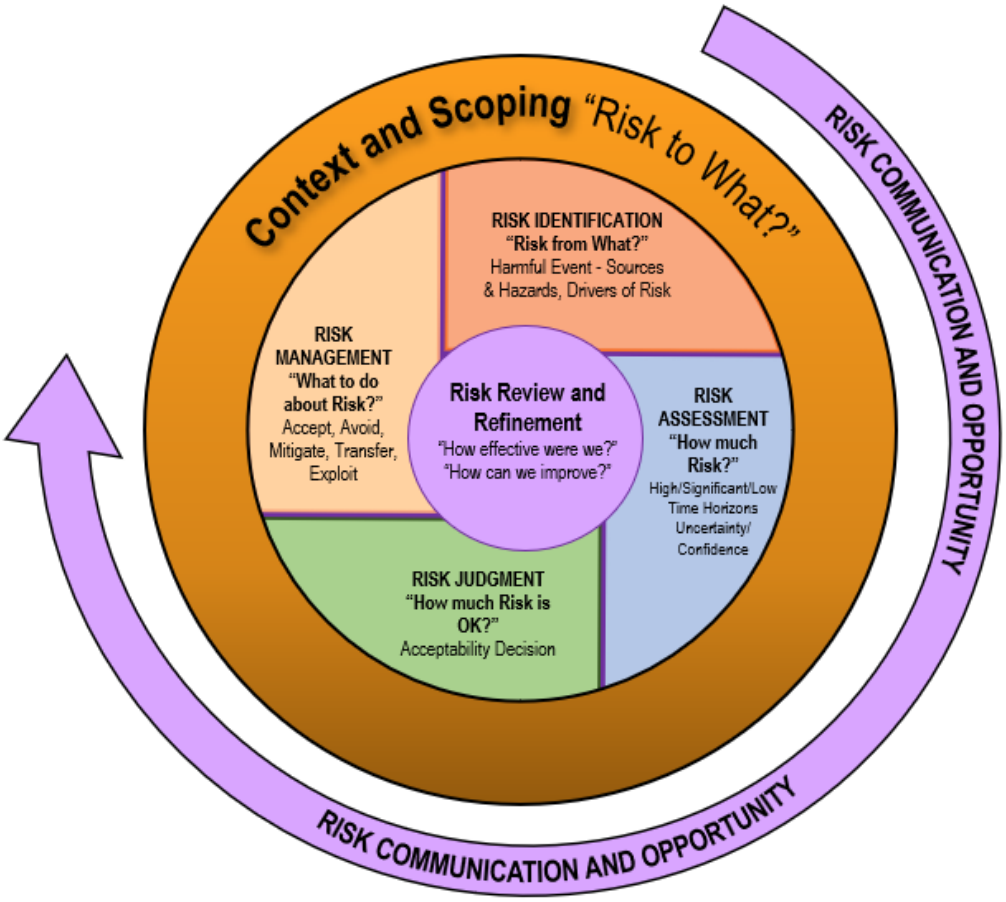


Figure 2. The Joint Risk Framework

3. JRAM Application

a. Context and Scoping. Before identifying risks (Pillar 1), commanders and their staffs must first establish the context and scope by answering the "risk to what?" question. The assessor coordinates with the appropriate Service Chief, Combatant Commander (CCDR), or Secretary of a Military Department—the authority ultimately responsible for managing the risk. Together, they define the standards (criteria, scale, terms, assumptions) and identify the stakeholders to involve in the assessment.

(1) Context and scoping define what is valued, how it may be affected over time, and the boundaries for examining risk. This process ensures that risk identification, assessment, judgment, and management are grounded in a shared understanding of the type of risk being assessed, the globally integrated environment, and the statutory responsibilities of the SecWar, Military Department Secretaries, CCDRs, and CJCS. The outcome is a documented risk context statement that outlines what is valued, the strategic setting, relevant time horizons, and the scope, roles, and scales for the assessment. Risk analysis is also inherently influenced by assumptions, and the risk context statement should document key assumptions and revisit them as necessary as new information emerges. To address urgent contingencies within an "immediate" time horizon (days to months), an expedited risk assessment process should be considered and tailored as appropriate. This streamlined approach enables rapid identification, assessment, and prioritization of risks while maintaining alignment with the established risk context and ensuring informed decision-making under time-sensitive conditions.

(2) This step should incorporate strategic thinking across time horizons to help senior leaders make risk-informed decisions aligned with overall strategy. The three time horizons from the JSPS continuum—near-term (0–3 years), mid-term (2–7 years), and long-term (5–15 years)—provide the framework for this approach. Ignoring these time horizons can hinder efforts to adapt and innovate the Joint Force, making it difficult to gain necessary advantages over adversaries and to compare risks across commands, functions, and domains.

(3) Lastly, context and scoping must account for interdependence among CCMDs, Services, allies, partners, and non-military (e.g., commercial) entities. A globally integrated perspective is essential, considering how events in one area of responsibility or domain might impact other regions or domains.

Risk Context Statement

a. Strategic Context. This assessment examines [MSR/MR] associated with [describe objectives, interests, missions, or plans], as directed by [NSS/NDS/NMS/DPG/ GEF/other]. The focus is on [brief description of "things of value"—e.g., deterrence posture, ability to defend X, force readiness, alliance cohesion] in a globally integrated context involving [CCMDs/functions/theaters/allies/partners/other stakeholders].

b. Time Horizons. Risk will be assessed across the following time horizons, consistent with JSPS usage:
– Near-term (0–3 years)
– Mid-term (2–7 years)
– Long-term (5–15 years)

c. Scope and Boundaries. This assessment covers [describe activities, missions, plans, capabilities, and forces in scope]. The geographic, functional, and operational scope includes [regions, domains, functions, or specific problem sets]. Interdependencies with [other CCMDs/functions/allies/partners/USG stakeholders] will be considered where they materially affect risk.

d. Roles and Responsibilities. The risk owner for this assessment is [title/ organization], accountable for decisions regarding acceptance, avoidance, mitigation, or transfer of risk.

e. Assumptions and Constraints. This assessment is based on the following key assumptions: [A1, A2, A3…] and constraints: [B1, B2, B3…]. Critical dependencies that could materially change the risk if altered include [C1, C2, C3…]. Related risks will be grouped into [issues] to capture aggregation and interaction effects across [commands, functions, time horizons].

f. Risk tolerance and Expected Outputs. Initial risk tolerance for this problem set is described as [qualitative statement—e.g., "willing to accept moderate, trending down risk to X in the near term to prevent significant risk to Y in the mid-to-long term"], subject to refinement during risk judgment and review. Outputs from this assessment are intended to inform [Chairman's Risk Assessment/readiness reporting/global force management decisions/ planning guidance/other JSPS products] and/or to support [specific title 10/statutory or planning requirements].

Figure 3. Risk Context Statement Example

b. Risk Identification (Pillar 1). After completing context and scoping, commanders and their staffs identify specific events and conditions that could harm what is valued defined in the risk context statement. Risk identification translates the strategic context into a structured set of potentially harmful events, along with their associated sources of risk and key drivers that may influence these events across time horizons. Risk identification should

consider events arising from both action and inaction—by the Joint Force or others. This includes scenarios such as not shifting posture, not investing in a capability, or not accepting near-term risk to mitigate greater future risk.

(1) Harmful Event. A harmful event is a foreseeable occurrence or condition that, if it happens, will negatively impact what is valued in the risk context statement. Examples include failure to achieve a strategic objective, degradation of a critical capability, or increased risk to the force. Harmful events may result from single episodes or from cumulative effects over time.

(2) Sources of Risk. Threats or hazards that—individually or in combination—have the potential to harm what is valued.

(a) Threat. State or non-state actors that possess the capability and intent or potential intent to harm what is valued, whether through military, informational, economic, cyber, or other means.

(b) Hazard. Conditions—internal or external to the DoW—that can enable or amplify harm or advantage. Hazards may include security, environmental, economic, demographic, technological, political, social, organizational, or other structural factors within or beyond the Joint Force.

(3) Drivers of Risk. Factors that influence the probability or consequence of risks arising from various sources. Drivers can increase or decrease risk by shaping the environment in ways that enable or minimize harmful events. Drivers should be considered across time horizons, as a driver that increases risk in one time horizon may become obsolete or reduce risk in another. Drivers may be internal or external to an organization, with examples provided in Figure 4. Other considerations for risk drivers include, but are not limited to:

(a) Frequency. The number of times a threat or hazard occurs within the situational environment over a given time horizon.

(b) Vulnerability. The susceptibility of an asset, force, or mission to face harm from a threat or hazard (e.g., due to weaknesses in security, design, or resilience characteristics).

(c) Resilience. The ability to anticipate, withstand, adapt to, and recover from disruption. Resilience is defined by the concepts of redundancy—identical or nearly identical ways and means to accomplish the mission—and robustness—the level of protection or preparedness to withstand a threat or hazard.

(d) Criticality. The importance of, or degree of dependency on, what is valued.

(e) Accessibility. How easily a hostile force or capability can reach what is valued.

(f) Recognition. How easily what is valued can be identified by a hostile force or capability, including its significance to the Joint Force.

(g) Impact. How severe the damage is, including the secondary and tertiary effects of damage to what is valued.

(h) Resources. People, equipment, funding, locations, or ideas available to respond to a threat or hazard; that is, what the Joint Force will use to mitigate the threat or hazard and reduce risk.

(i) Response. The changing demands placed on the Joint Force, which may increase or decrease as situations escalate or de-escalate. The situational environment is constantly changing in response to Joint Force actions, adversary actions, and environmental factors.

(j) Reliance. Reliance on commercial capabilities can provide opportunities beyond organic capabilities and is often identified as a risk management measure. However, it may also introduce risk. Understanding the scope and impact of Joint Force reliance on external entities and capabilities is necessary to fully inform risk assessment, judgment, and management.

Internal Driver Examples (Primarily within DoW Control)	External Driver Examples (Primarily Outside DoW Control)
Force posture and presence decisions	Adversary capabilities, intent, and risk appetite
Readiness levels, training, and modernization choices	Allied and partner capacity, access, and political will
Redundancy and resilience of networks, basing, and logistics	Global economic, technological, environmental, or demographic trends
Talent, manning, and rotation policies	Domestic and international political conditions and legal constraints
Allocation of resources among campaigns, theaters, and portfolios	Actions by other USG departments and agencies or non-state actors

Figure 4. Examples of Internal and External Risk Drivers

(4) Aggregation. When appropriate, events and issues can be combined to describe the overall risk to a strategic objective, mission set, or force element. Aggregated risks should retain enough detail to support targeted mitigation efforts and the development of opportunities. Assessors can link multiple risks to analyze how their aggregation could alter the overall risk landscape, as described below. Risk aggregates at higher echelons, and risk assessments should inform risk management decisions at each echelon. However, risk must also be reported to higher echelons when appropriate—both because higher echelons may be better positioned or resourced to address risks and to inform their own risk assessments. Risk evaluated as acceptable at one echelon may be judged unacceptable when aggregated at higher levels.

Example Aggregated (Complex) Risk Statement
(Can be used when multiple related harmful events drive a single risk judgement)

"If the following related harmful events or conditions occur in combination within [Time Horizon], [Event/Condition 1, Event/Condition 2, Event/Condition 3*], then the Joint Force's ability to* [execute mission/maintain posture/etc.] *may be* [degraded/denied] *resulting in* [risk] *to* [thing of value] *in the* [time horizon]."

The events or conditions aggregated should each be assessed individually before being aggregated into a complex risk.

Figure 5. Example Aggregated (Complex) Risk Statement

c. Risk Assessment (Pillar 2). Building on the risk context statement and the outputs of risk identification (Pillar 1), commanders and their staffs conduct risk assessment to assign probability and consequence levels and describe trends over time. This pillar establishes the **baseline** risk levels that inform subsequent risk judgment (Pillar 3) and risk management (Pillar 4).

(1) Probability and Consequence. After identifying the known sources and drivers of risk, commanders and their staffs conduct risk assessment to estimate the probability of identified events occurring and their potential consequence on what is valued, across time.

(a) Probability

1. Probability (P) is the assessed likelihood that a harmful event will occur within a specified time horizon under the conditions outlined in the risk context statement. To ensure clear and unambiguous risk communication, probability should be defined in a quantifiable manner. A four-level table is typically used to help assessors designate the probability level of an event

occurring (Figure 6). Note: The probability boundaries in the table should be considered best estimates during qualitative risk assessment.

Probability of Event (P)
Very Likely (~81-99%)
Likely (~51-80%)
Unlikely (~21-50%)
Very Unlikely (~01-20%)

Figure 6. Probability Levels

2. The levels "Very Likely" and "Very Unlikely" are assigned smaller probability ranges to reserve them for events with a higher degree of certainty—those more certain to happen or not happen. The "Likely" and "Unlikely" levels capture outcomes with less certainty. The structure deliberately omits a level for very low, zero, or negligible probability. While a strategy and force structure that operates without risk may be ideal, moving from "Very Unlikely" to zero probability could require an exponential increase in resources. Given that resources are finite, commanders and staffs must manage risk efficiently through risk management. Note: When appropriate, assessors should consider confidence—an expression of the strength of information, the assumptions that underpins analysis, and the degree of gaps (see paragraph 4.a.(c) in Enclosure C for more on confidence).

(b) Consequence

1. Consequence (C) refers to the impact or resulting harm if the event occurs. Like probability, consequence should be clearly defined to ensure unambiguous risk communication. A four-level table (Figure 7), ranging from "Extreme" to "Minor," helps assessors designate the level of consequence for an event. These levels should be tailored to specific risk scenarios, with harm generally estimated by considering risk drivers such as vulnerability, resilience, criticality, impact, and resources.

Consequence of Event (C)
Extreme harm to the thing of value
Major harm to the thing of value
Modest harm to the thing of value
Minor harm to the thing of value

Figure 7. Consequence Levels

2. For example, “modest harm” might mean that the current mission or force can achieve all critical objectives with acceptable costs, while “major harm” could mean that only the most critical objectives are achieved, but at substantial costs (more detailed examples are provided in Figure 22). For beneficial events, consequence assessments capture the extent to which the event would create or enhance advantages for the Joint Force or the nation.

3. Consequence assessments should consider the effects on:

a. Achievement of strategic objectives and missions.

b. Risk to the force, including readiness, resilience, and survivability.

c. “Risk from the force,” including second and third-order consequences of military action related to diplomatic, economic, or information domains.

d. Deterrence credibility, alliance and partner cohesion, and broader national interests as applicable.

e. Other dimensions identified in the context statement (for example, escalation risk, domestic support, or industrial base resilience).

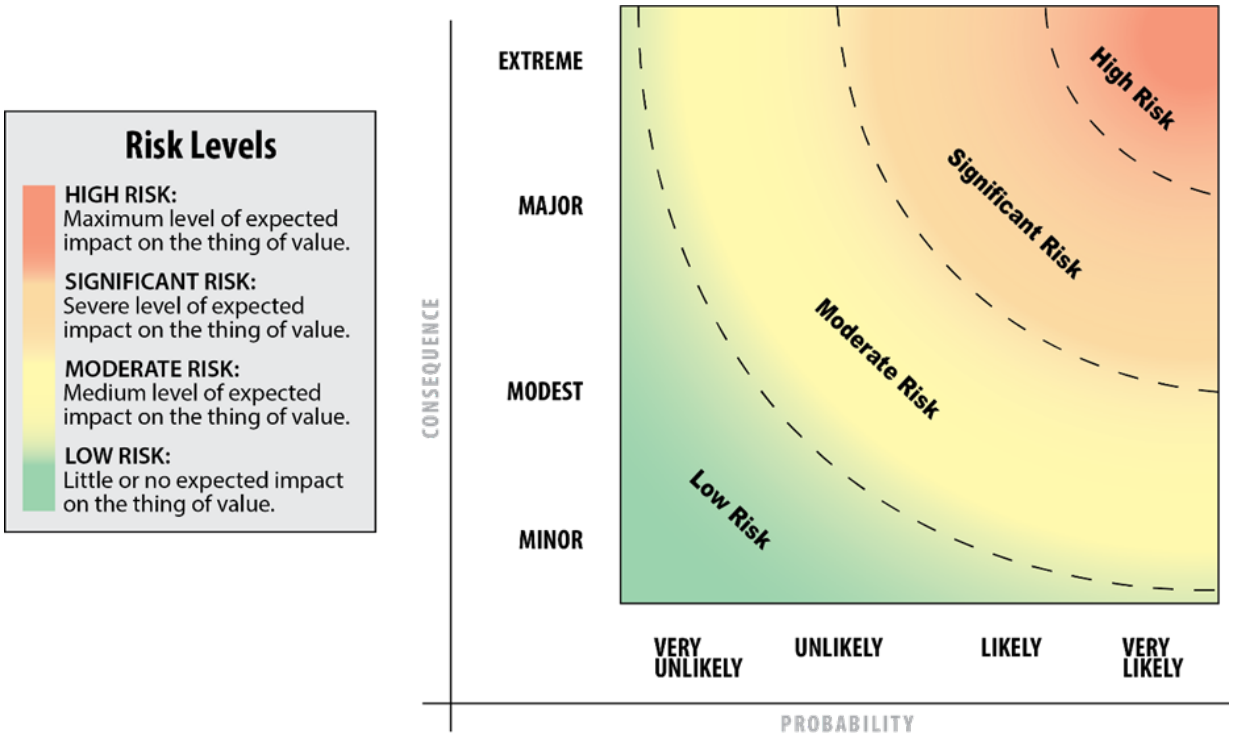


Figure 8. Baseline Risk Levels and Generic Risk Contour

(2) Risk Characterization. Risk characterization assigns a risk level to each potential threat or hazard based on the previously assessed probability and consequence. Plotting these factors on a risk contour graph helps determine an initial baseline risk level. Figure 8 illustrates the baseline risk levels—*Low*, *Moderate*, *Significant*, and *High*—which should remain consistent across Joint Force risk assessments.

Risk = Probability x Consequence

Adhering to the risk contour in Figure 8, a harmful event is assessed with a "Very Likely" probability and "Minor" consequence is characterized as a *Low* or *Moderate* risk. Separately, a harmful event with "Very Unlikely" probability and "Extreme" consequence is also a *Low* or *Moderate* risk. While the risk levels may be the same, it is important to include the probability and consequence levels when communicating to the risk owner. See the Risk Communication component for more information.

Figure 9. Risk = Probability x Consequence

(3) Trend Modifiers. Risk levels can incorporate a temporal aspect by assigning "trending up" or "trending down" modifiers to the baseline risk level. These modifiers indicate the assessed direction of risk over a specified time horizon if left unmanaged, reflecting the intersection of probability (X-axis), consequence (Y-axis), and time (Z-axis). This approach is particularly useful for communicating risks that persist over the assessed time horizon. For example, a risk characterized as "*Significant trending up*" in the near term (0–3 years) suggests that the risk is currently *Significant*, is growing, and could potentially become *High* by the end of the third year. Trend modifiers of "*High trending up*" or "*Low trending down*" indicate whether said risk is increasing or decreasing in scope. For example, *High trending up* indicates that a risk already categorized as *High* and is continuing to get worse and should be explained in a risk statement. Trend judgments consider factors such as:

(a) How drivers and sources of risk are expected to evolve over time.

(b) The projected effects of planned actions and resourcing decisions, as well as the potential consequences of inaction.

(4) Time. The time horizon is crucial for balancing risk over time. Decisions made to manage risk today will influence future risk exposure. Conversely, focusing on mitigating potential future risks may increase risk in the present or near term.

(a) Figure 10 provides a generic visual example of how risk levels

may decrease over near-, mid-, and long-term time horizons (e.g., *High trending down*). As this graphic illustrates, risk is not linear and should not be constrained by linear thinking. Decision-makers must consider the trending direction of risk when deciding whether to accept, avoid, mitigate, or transfer it (Pillar 4). It is also important to remember that uncertainty increases as time horizons expand in risk assessment.

(b) Figure 10 depicts how risk may change over the near-, mid-, and long-term time horizons. In the near-term (0–3 years), there is a Very Likely probability and Extreme consequence to a harmful event occurring. Moving through time on the z-axis, the risk of the harmful event occurring is reduced through risk management. By the mid-term (2–7 years) time horizon, there is Likely probability and Modest consequence to a harmful event occurring. In the long-term (5–15 years), the probability and consequence of the harmful event occurring is reduced further to Very Unlikely probability and Minor consequence. The increasingly transparent risk levels represent how the probability and consequence of risk may become less certain over time.

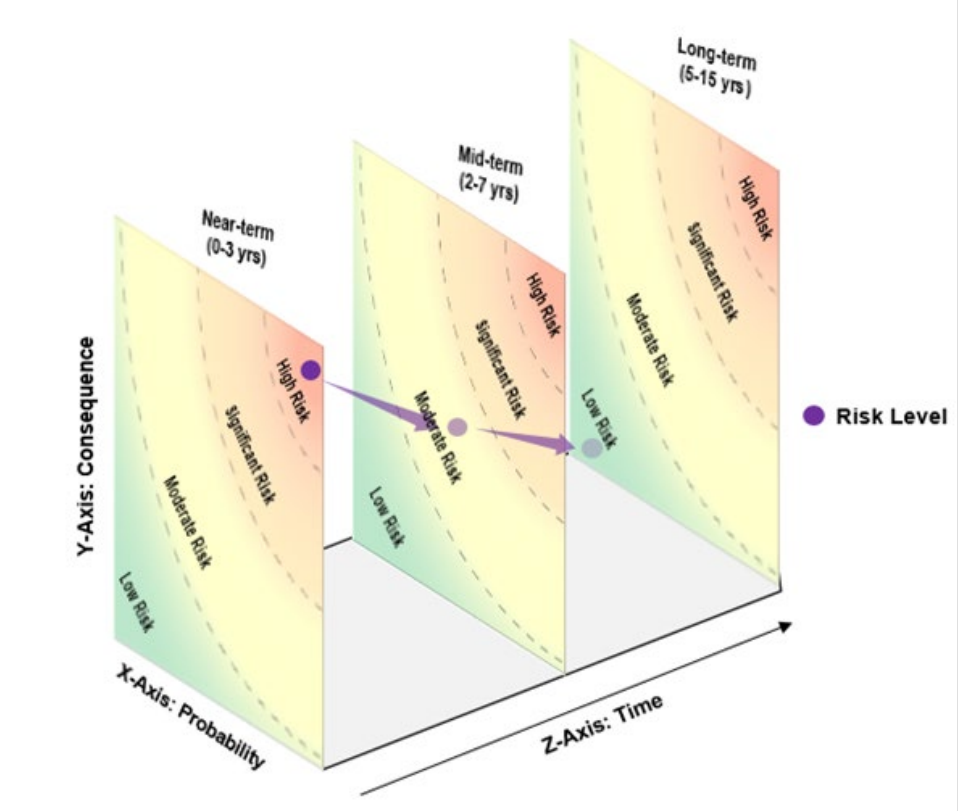


Figure 10. Risk Across Strategic Continuum Time Horizons

d. Risk Judgment (Pillar 3). Risk judgment is a qualitative process focused on determining the degree of acceptable risk for decision-makers. Using the

baseline risk levels and trend modifiers from Pillar 2, commanders and their staffs evaluate whether the risk is acceptable in the context of strategic guidance, national and military objectives, and the commander's risk tolerance. This evaluation should be factually supported to enable informed decision-making at the appropriate level of responsibility. The outcome of this pillar is an accepted risk profile that guides risk management decisions and serves as a foundation for future review and refinement (Pillar 5).

(1) Risk Evaluation

(a) During risk evaluation, a decision-maker judges the acceptability of a risk, which informs how the risk will be managed (Pillar 4). This process allows decision-makers to manage risk in a way that maintains an advantage. They will weigh risk in a globally integrated manner across near-, mid-, and long-term time horizons, understanding that reducing risk in one area or time horizon may lead to increased risk in another. For example, a decision-maker might choose to accept more "Likely (P), Modest (C)" events rather than "Very Unlikely (P), Extreme (C)" events from the same threat, even if both fall within the same *Moderate* risk contour (as shown in Figure 8). This process aims to guide leaders toward taking calculated risk—**the conscious acceptance of potential assessed negative impacts of a decision to seize initiative, gain advantage, or accomplish the mission**.

(1) Acceptable. Risk that the commander determines can be accepted without additional mitigation at this time.

(2) Unacceptable. Risk that the commander determines is too high to accept without specific actions to avoid, mitigate, transfer, or otherwise manage it.

(b) In making this determination, risk judgment considers:

(1) The type of risk (MSR, MR to mission, MR to force) and the objectives, missions, and forces affected.

(2) The time horizon(s) over which risk manifests and the potential for near-term decisions to increase or decrease risk in the mid-/long-term.

(3) The trend (for example, a *Moderate* risk in the near-term trending up toward *Significant* in the mid-term) and whether existing or planned actions are sufficient to change that trajectory.

(4) Key tradeoffs, opportunity, and opportunity cost, including where accepting higher risk in one area or time horizon reduces risk elsewhere,

and where failing to pursue an opportunity would forgo meaningful advantage within the commander's stated risk tolerance.

e. Risk Management (Pillar 4)

(1) This pillar focuses on designing, implementing, and monitoring the outcomes of risk decisions. Risk management translates risk judgments into concrete actions—or deliberate inaction—by selecting options to accept, avoid, mitigate, or transfer risk, and then assessing the resulting residual risk across time horizons. Residual risk is the risk that remains after a decision-maker has chosen a COA. It is important to acknowledge that zero risk is unattainable as long as threats or hazards exist. Risk management decisions are made within the context of strategies, policies, operations, or tactics, with careful consideration of the various drivers of risk to guide decision-making.

(a) Accept. Make an informed decision to act without conducting risk mitigation efforts.

(b) Avoid. Forgo the activity that would produce unacceptable risk or remove what is valued that could be damaged due to unacceptable risk.

(c) Mitigate. Implement measures that decrease the probability or consequence of harm across time horizons.

(d) Transfer. Take action to change when and where the risk is incurred and potentially who or what incurs it.

(2) Risk of Inaction. All risk analysis is designed to inform decision-making, whether the choice is between a single action, multiple actions, or action and inaction. The choice between action and inaction is not just about the immediate benefits or losses; it also involves acknowledging what could have been achieved in the future had one chosen to act. Inaction can lead to missed opportunities, stagnation, or failure to respond to a growing or anticipated threat, leading to an increase in the risk faced.

(a) Action. Decisions and measures taken by the Joint Force or other stakeholders that alter force structure, posture, plans, readiness, resources, concepts, or behavior in ways that affect risk.

(b) Inaction. The deliberate decision not to change force structure, posture, plans, readiness, resources, or other factors when such changes are feasible. Inaction can preserve, increase, or, in some cases, avoid creating risk.

(3) Opportunity Cost. In the context of military risk analysis, opportunity cost is the value of the next-best alternative that is foregone when a decision is made to allocate resources to a specific COA. Simply put, it is **the cost of the lost opportunity**. This concept is critical in defense planning because resources such as funding, personnel, and materiel are finite. Every decision, from budgetary appropriations to the deployment of a single unit, involves trade-offs due to the fundamental principle of resource scarcity. By choosing to do one thing, decision-makers inherently choose **not** to do something else, and the value of that "something else" is the opportunity cost.

f. Risk Review and Refinement (Pillar 5). Pillar 5 focuses on evaluating the effectiveness of previous risk assessments, judgments, and management actions over time, using these insights to enhance future risk processes. This pillar involves comparing expected and observed outcomes, assessing the accuracy of probability and consequence judgments, reviewing the effectiveness of risk mitigations, and refining assumptions, scales, and risk tolerance as needed. By closing the loop in the risk cycle, this process ensures that the Joint Force becomes more accurate, adaptive, and disciplined in managing risk. During ongoing operations, review and refinement should occur in stride, not after the fact. Assessors should establish a regular battle rhythm to revisit key risk statements, update metrics as new data becomes available, and record major changes and their drivers for later lessons-learned analysis.

(1) Purpose and Linkages. Review and refinement leverage information from monitoring, risk reporting, and decision outcomes to test and refine the outputs of Pillars 1–4. This process can be conducted as a discrete activity, such as during annual assessments like the CRA, or as a continuous practice embedded within existing battle rhythms.

(2) Review of Risk Assessments and Judgments. Commanders and their staffs should periodically review selected past risks, particularly those assessed as *High* or *Significant*, judged unacceptable, or associated with major decisions in areas such as strategy, posture, readiness, or resourcing. For each of these risks, the review should, at a minimum:

(a) Compare expected outcomes (probability, consequence, and trend recorded in Pillar 2) with observed outcomes over the applicable time horizons.

(b) Identify instances where risk was overestimated, underestimated, or correctly characterized, and identify what process or logic improvements can be made in conducting future risk assessments.

(c) Identify what drivers of risk contributed to the event occurring or

failing to occur. Were those drivers known or monitored? Were some drivers more impactful than others?

(3) Review of Risk Management Actions. Review and refinement also involve assessing the effectiveness of risk management actions documented in Pillar 4. For each major acceptance, mitigation, avoidance, or transfer, the review should evaluate:

(a) Whether planned actions were implemented as intended.

(b) How these actions impacted risk in other missions, regions, or time horizons (e.g., did mitigation in one area generate risk elsewhere?).

(c) Any necessary adjustments to assumptions, probability and consequence assessments, and risk tolerance.

(d) Which risk drivers had the biggest impacts or contributions and where reduced gaps in knowledge may have contributed to less uncertainty in the assessed risk.

(4) Integration into Future Risk Work. Lessons learned in Pillar 5 can be integrated into future applications of JRAM by updating risk context statements and risk identification guidance (context and scoping and Pillar 1) to reflect a refined understanding of what is valued, where risk is likely to emerge, and which drivers matter most. These lessons can also inform future risk assessments (Pillar 2), shape future risk judgment (Pillar 3), and refine risk management practices (Pillar 4). Where appropriate, review and refinement findings should be shared to promote Joint Force learning and foster a common understanding of risk.

g. Risk Communication (Continuous Component). Risk communication is central to any successful effort to appraise and manage risk and must be continuous throughout JRAM execution. Effective communication among risk stakeholders helps reduce misunderstandings and potential surprises. For instance, identifying sources and drivers is essential for contextualizing the risk of a given event. Communicating these drivers, along with any assumptions, as early as possible ensures that all stakeholders understand the scope of the risk involved. This is crucial for enhancing dialogue and building confidence in the outcomes. This manual standardizes a common risk lexicon to facilitate effective communication. Senior leaders must provide detailed analysis when communicating risk levels such as *Significant* or *High*.

(1) Risk Statement. A risk statement should clearly express probability, the harmful event, time horizon, key drivers, consequence, overall risk level,

and trend. A recommended template appears in Figure 11.

Template for Writing an Effective Risk Statement

"There is a [*probability level*] probability that [*harmful event*] in the [*time horizon*], driven primarily by [*key drivers*] under current [*action/inaction/posture/plan*] conditions, will result in [*consequence level*] consequence. This results in [*risk level*] [*risk type*] to [*thing of value*]".

For example: "There is a 'Likely' probability that a major regional crisis in the near-term (0–3 years), driven primarily by adversary military growth, limited partner capacity, and delayed posture adjustments under current employment and resourcing plans, will occur with 'Major' consequence. This results in *Significant*, *trending up*, Military Risk (Risk-to-Mission) to executing the *National Military Strategy* [Objective] in the U.S. Pacific Command area of responsibility."

Figure 11. Template for Writing an Effective Risk Statement

h. Risk Opportunity (Continuous Component)

(1) Throughout each pillar of the JRAM, assessors should actively consider how risk identification, assessment, judgment, and management can reveal opportunities that provide a relative advantage. This begins with the identification and assessment pillars (Pillars 1 and 2), where assessors should examine risks with an eye toward uncovering potential opportunities. However, the opportunity lens is most impactful in the judgment and management pillars (Pillars 3 and 4). Opportunity is not the absence of risk, but the space for decision-makers to proactively offset or exploit risk associated with a harmful event to maintain advantage.

(2) In theory, if decision-makers accurately determine the degree of acceptable risk and manage it effectively, they can simultaneously create space for opportunities that align with strategic priorities and achieve key milestones. By moving through the risk analysis process with a focus on opportunity, the Joint Force is encouraged to continuously seek ways to make decisions that reflect a global perspective of defense priorities. Risk is not solely the presence of a threat; it can also create or expose opportunities that can be strategically exploited.

(a) Beneficial Events. A beneficial event is a foreseeable occurrence or condition that, if it happens, will positively impact what is valued. Examples include strengthened deterrence, improved partner capacity, or increased operational access. Identifying beneficial events allows for the consideration of risk opportunities, including situations where accepting or exploiting risk can create or amplify advantage. Beneficial events (e.g., successful campaigns or

favorable political shifts) can result in "catastrophic success," creating new sources of risk to be identified and assessed.

(b) Exploitation of Risk. Consider the "upside" of risk by deliberately accepting or rebalancing risk **to pursue opportunities that can create or enhance advantage**. Viewing risk as an opportunity is a continuous process, encouraging decision-makers to identify and exploit potential benefits while managing associated risks. Where beneficial events or opportunities for exploitation have been identified, risk statements can also express potential advantage and the risk of failing to pursue it (Figure 12).

Template for Writing an Effective Opportunity Statement

"There is a [*probability level*] probability that [*beneficial event/opportunity*] in the [*time horizon*], if [*key actions/conditions*] are undertaken, will generate [*consequence level – beneficial*] improvement in [*thing of value*]. If not pursued, this creates [*risk level*] risk to [*risk type*]."

For example: "There is a 'Likely' probability that implementing a forward posture and integrated exercise concept in the mid-term (2–7 years), if adequately resourced and coordinated with allies and partners, will generate 'Major' (beneficial) improvement in deterrence credibility and operational access.

Figure 12. Template for Writing an Effective Opportunity Statement

i. Other Considerations. Several major challenges to successful risk analysis exist:

(1) Complexity. "How do my risks relate and compound?" Establishing cause-and-effect relationships and accounting for intervening variables can be challenging. In complex systems with multiple sources and drivers of risk, the overall risk level may be higher than the sum or average of individual risks due to synergistic effects.

(2) Uncertainty and Ambiguity. As human knowledge is inherently incomplete, stakeholders may have differing views on the exact problem or sources of risk resulting from multiple legitimate interpretations. Additionally, the future strategic environment is subject to randomness, leading to potential deviations that cannot be accurately modeled using probabilistic analysis. Therefore, when determining a risk level, it is more accurate to visualize the risk as having a small amount of variance, represented as an ellipse rather than a precise point on a risk contour graph. As the time horizon expands, the degree of uncertainty increases as shown in Figure 8.

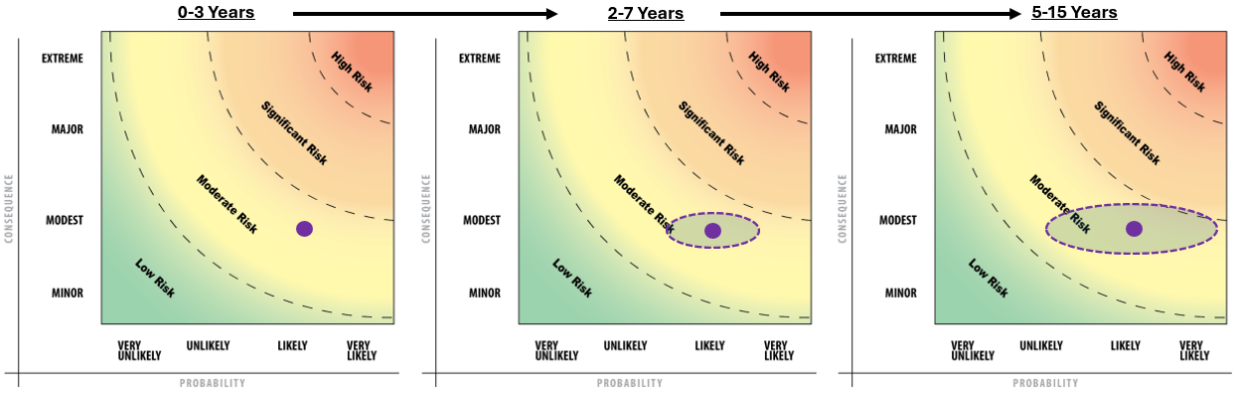


Figure 13. Visualizing Risk Uncertainty Across Time

(3) Volatility. "How fast is my risk changing? How is this likely to change my assessment?" The rapid rate of environmental change can make even the most current data inadequate for decision-making. Volatility tends to decrease as risk is assessed at levels above the tactical echelon.

(4) Bias. "Who has challenged my key assumptions and helped identify biases?" Assessors may be influenced by various cognitive biases during risk analysis. Awareness of these biases helps refine the process toward greater objectivity. Explicitly identifying assumptions allows for bias review. Bias can be countered by involving multiple stakeholders in reviewing assumptions and assessments, by using a "devil's advocate" to challenge assumptions, or by assessing the event as an element of a broader system instead of as an isolated event.

(5) Allies and Partners. "How might interaction with or from my partners affect my risk?" Relationships with allies, partners, and non-military entities can both increase and decrease risk. Allies and partners may increase risk if they are unwilling, unable, or choose not to manage their own risk, leading to greater vulnerability for U.S. military objectives. Conversely, they may decrease risk by identifying gaps in risk assessments and assisting in risk management. Leveraging existing entities beyond forces support may also expand opportunities, approaches, and capabilities beyond the organic force to achieve outcomes that the Joint Force cannot achieve alone.

(6) Global Integration. "How will my actions affect the missions and risk of others?" A globally integrated approach to risk is fundamental to understanding how any given risk response implemented by one CCMD or Service may increase or decrease risk for another (Figure 14). Leaders must be intentional about how they choose to accept, avoid, mitigate, or transfer risk to align with strategic priorities. Strategic guidance may direct one CCMD or Service to accept increased risk if it can better address it or if that risk is a

lower priority compared to others. In this way, risks may be prioritized in a constrained resource environment to align with strategic priorities. A globally integrated approach to risk emphasizes the need for communication both up and down and across the chain of command to ensure risk analyses across CCMDs and Services are not examined solely in isolation.

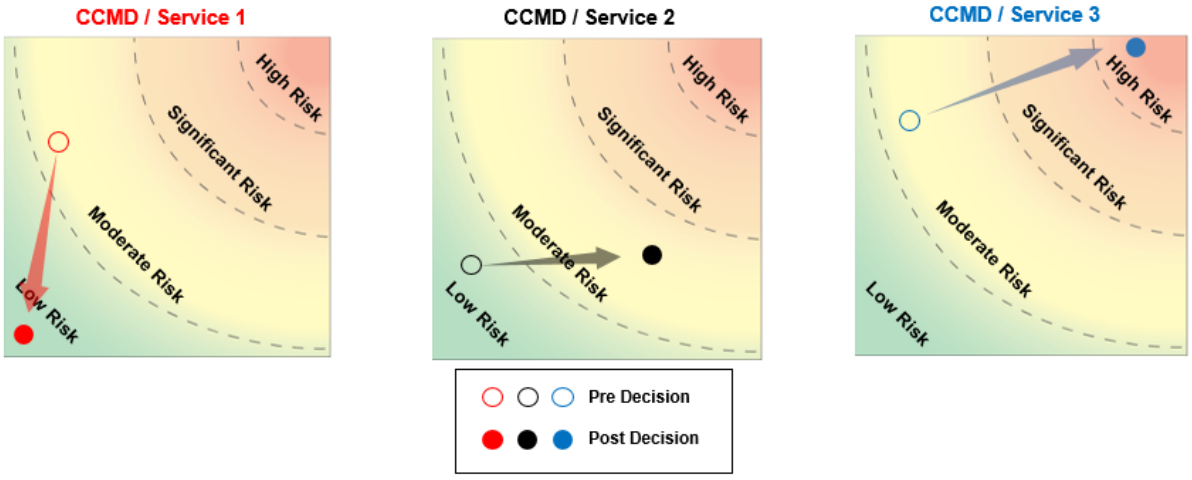


Figure 14. Globally Integrated Approach to Risk

(a) Figure 15 combines a globally integrated approach to risk with time horizons, affording an assessor or senior leader the ability to visually understand how risk decisions affect the Joint Force as a whole. In this example, the decision to lower risk for CCMD 1 in the current time horizon leads to a subsequent increase in risk from CCMD 2 and Service 1. Of greater note, risk to Service 1 will continue to increase across time horizons reaching *High* risk in the third time horizon.

(b) Managing risk proactively may provide decision-makers the opportunity to consider how it can influence drivers and risk in subsequent time horizons. It also provides decision makers with the opportunity to carefully weigh risk across the Joint Force and ensure alignment with strategy. It is important to remember that leaders are often incentivized to prioritize near-term risk. Decisions taken to reduce near-term risk can increase risk in the future (e.g., delaying modernization, over-use of forces, deferred investment). Risk assessments should consider how decisions shift risk across time horizons.

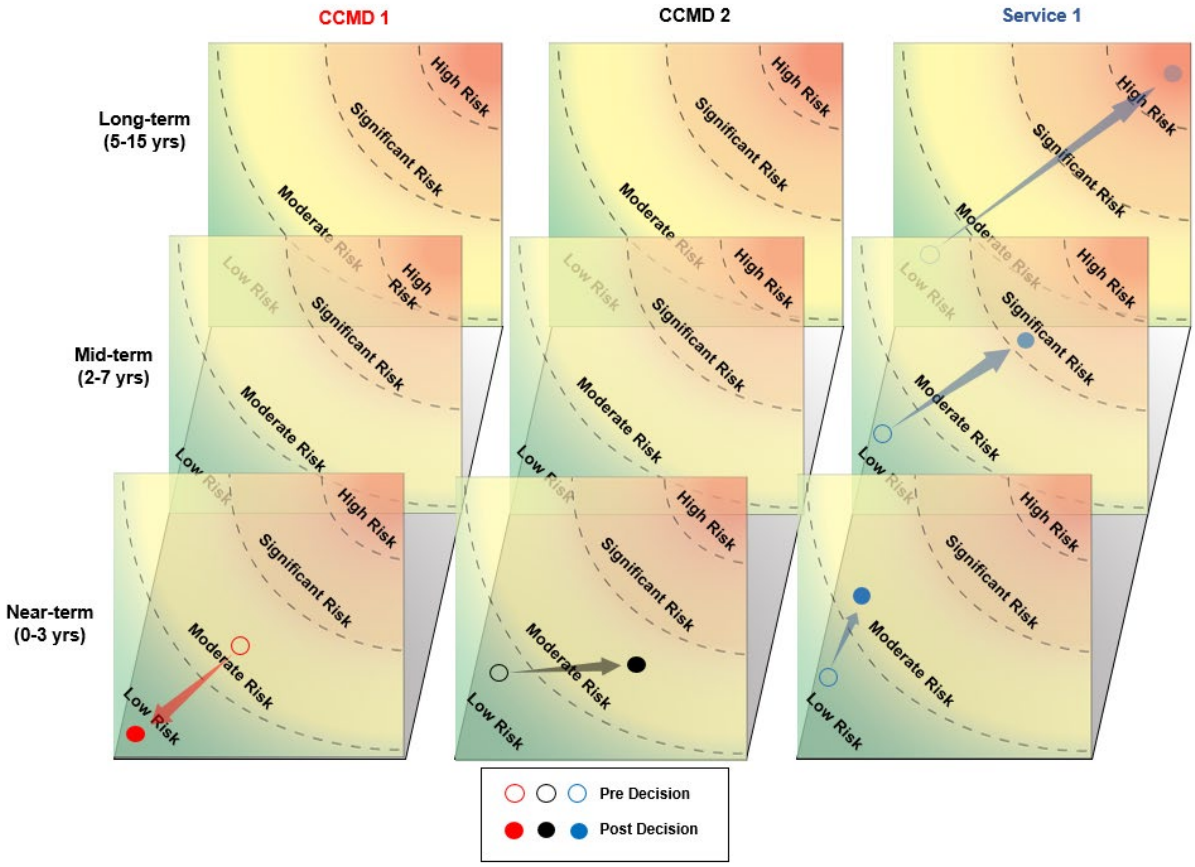


Figure 15. Globally Integrated Time Horizons

(c) The considerations explained above are why decision makers' judgment and experience are critically important within the risk analysis methodology. The senior leader or commander can often provide a distinct and broader perspective or apply strategic intuition that helps determine the appropriate risk decision. A senior leader's clearly articulated risk assessment (quantifiable where appropriate) improves the overall understanding and communication of risk, ensuring that risk is comparable across regions, functions, and domains and over time.

(7) Accumulated Risk. While aggregated (overall) risk is derived from a single practitioner's various risk inputs—MSR and MR (RM and RF)—accumulated risk accounts for a macro view of the risk environment, specifically regarding past risk decisions. The current risk environment should be viewed in context of past decisions, not in isolation from the past. For example, the decision to transfer an asset from one theater to another carries a snapshot of risk. This model does not always account for the accumulated risk impact of previous posture decisions to transfer similar assets from the

notional theater in question and how acceptance of those risks has accumulated over time.

(8) Temporal Consideration of Risk Decisions. The outcomes of risk decisions are not always realized immediately, with the impacts often stretching across years. When making risk decisions, leaders should consider the periodicity of impact that these decisions will have in the future. This can be visualized in Figure 16, where we note that past decisions have shaped the environment in which we operate now and should be considered in the future. (Definitions of the risk types noted below can be found in Enclosure C).

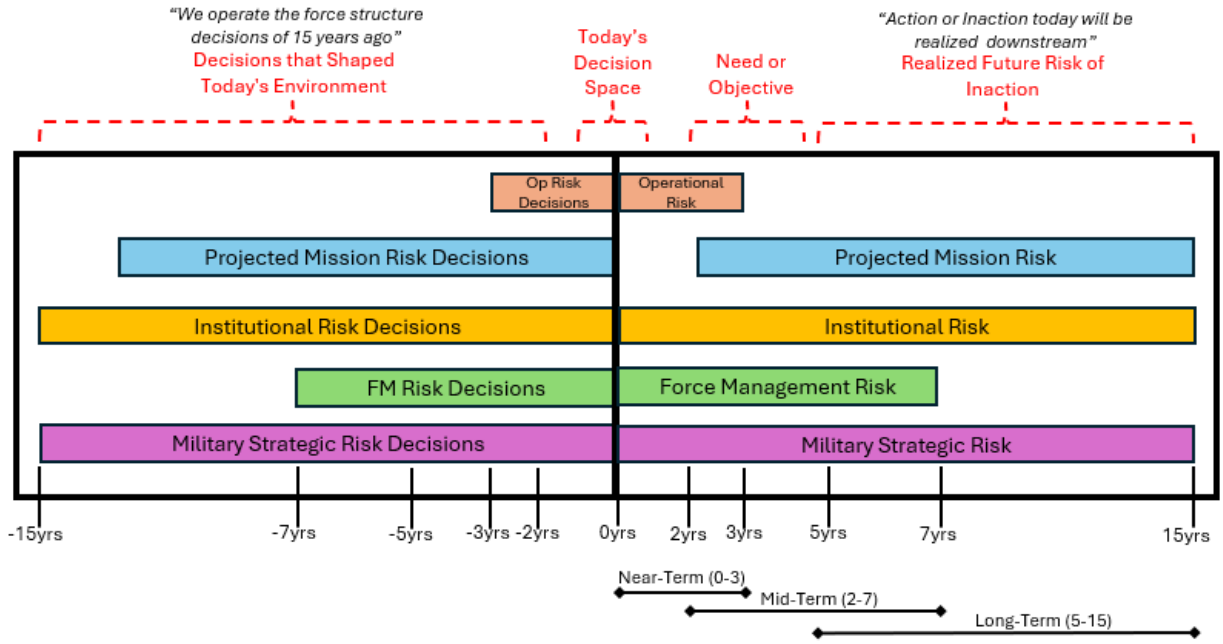


Figure 16. Downstream Effects of Risk Decisions

(9) Quantitative Risk Analysis in Military Operations. The JRAM is primarily a structured qualitative framework that uses common scales and clear assumptions while drawing on quantitative information where available and appropriate to inform probability and consequence judgments.

(a) Quantitative risk analysis is a data-driven approach that uses numerical and statistical models to assign a value to risk. In a military context, this value is typically expressed in terms of its potential impact on key mission parameters, such as the probability of mission success, projected casualty rates, equipment loss expectancies, or anticipated delays in a critical phase of an operation. This method provides an objective measure of the potential impact of risks and is best employed when reliable data is available and a high degree of analytical rigor is required.

(b) Quantitative analysis is especially useful when:

1. Sufficient, reliable data and validated models exist for key variables.

2. A high degree of analytic rigor or precision is required (e.g., major investment, force structure, or posture decisions.)

3. Alternative COAs must be compared on a common numerical basis (e.g., expected loss, time, or cost).

(c) Quantitative approaches should still account for uncertainty and model limitations, and their outputs are used to inform, not replace, commanders' judgment in Pillars 2 and 3.

Method	Pros	Cons
Qualitative Analysis	**Rapid Assessment:** Ideal for time-sensitive decisions.	**Subjectivity:** Results are based on perception and can be influenced by bias.
	Simplicity: Accessible to leaders at all levels without complex calculations.	**Lack of Precision:** Does not provide specific, numerical impact data, making it hard to compare different risks or justify resource allocation.
	Prioritization: Quickly identifies and categorizes the most significant threats.	
Quantitative Analysis	**Objectivity:** Provides a defensible, data-driven assessment based on measurable inputs.	**Data/Intel Intensive:** Requires significant amounts of credible data and intelligence.
	Detailed Insight: Offers a granular understanding of how threats can degrade mission capabilities.	**Time/Resource Intensive:** Can be complex and time-consuming, often requiring specialized tools and personnel.
	Analysis of Alternatives: Allows for concrete comparison of different countermeasures or Courses of Action.	**Illusion of Certainty:** Can create a false sense of certainty by producing a precise score that may not capture the variability of the real world.

Figure 17. Qualitative versus Quantitative Risk Analysis

ENCLOSURE C

RISK-TO-STRATEGY – STRATEGIC ASSESSMENTS

"The Joint Chiefs of Staff, in view of their global responsibilities and their perspective with respect to the worldwide strategic situation, are in a better position than any single theater commander to assess the risk of general war. Moreover, the Joint Chiefs of Staff are best able to judge our own military resources with which to meet that risk."

General Omar N. Bradley
First Chairman of the Joint Chiefs of Staff

1. Introduction

a. Enclosure B introduced the JRAM framework and described how an organization can adapt the pillars to fit their needs, using baseline risk levels (*Low*, *Moderate*, *Significant*, *High*) to ensure standardization across risk assessments and communication. This enclosure examines Risk-to-Strategy and guides the application of risk analysis across strategic planning assessments within the JSPS.

b. Risk-to-Strategy is the aggregate risk across the DoW enterprise that provides an assessment of the risks associated with the Joint Force's execution of the strategy. This should be recognized as markedly different from risk-of-strategy—the risk potentially introduced through implementation of strategy itself. Global Force Management (GFM) processes and the CRA are examples of processes that communicate Risk-to-Strategy aligned with the JSPS. Both the CRA and GFM processes have adopted the methodology framework from Enclosure B and can be used as examples for all Joint Force risk-related processes.

2. Joint Risk Analysis Methodology Application to Strategic Decision-Making.

The *National Defense Strategy* (NDS) sets the strategic direction for the DoW. SecWar military risk decisions through GFM processes seek to satisfy this strategic direction while using resources efficiently, and GFM decisions are a key part of this calculus. Central to these decisions is the need to balance military risk, an imperative driven by the fact that military forces are a finite resource. This military risk comprises two primary components: RM and RF. CCMDs advocate for understanding and mitigating RM, while the Services primarily advocate for RF. The Service components assigned to CCMDs act as the crucial conduit between these two perspectives, ensuring a holistic understanding of risk informs SecWar decisions.

a. GFM and the Secretary's Orders Book. In accordance with (IAW) the *Global Force Management Implementation Guidance* (GFMIG), GFM allocation sourcing

recommendations—with the associated risks—are presented to SecWar in the Secretary's Orders Book. Secretary's Orders Book timelines and procedures are detailed in reference (b).

b. Readiness Reporting. Readiness reporting is directly (and inversely) related to risk. As such, readiness assessments in Defense Readiness Reporting System and Status of Resources and Training System provide the foundation for risk assessments and impact of decisions related to resourcing and authorities, as well as the trade-offs between RM and RF. Readiness assessments also provide insight into ongoing and potential mitigation efforts.

c. Standardized Risk Language. Risk language used throughout the GFM processes is standardized to ensure clear and consistent communication across the Joint Force. Terms like "RM, RF, future military risk, and overall (aggregated) risk" are used. Effort should be made to avoid using generic, unclear, or otherwise non-standard risk language.

d. GFM Comparative Risk Analysis. The GFM processes present competing priorities, with associated risks, to senior leaders for management of those priorities in a risk-informed way. While existing models offer a snapshot in time of competing priorities and reflected risks, Figure 18 provides a notional example of how two CCMDs may be respectively affected by a proposed force transfer between the two. In this notional example, the force transfer results in decreased RM for U.S. Pacific Command during the deployment period, while reflecting the anticipated increase in RM incurred by U.S. European Command.

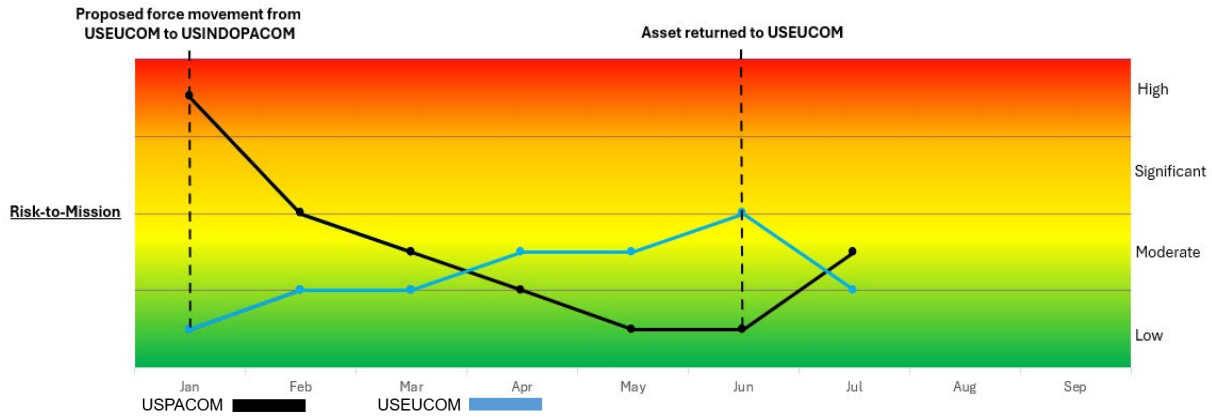


Figure 18. Notional Combatant Command Comparative Risk Analysis Across Time

3. Joint Risk Analysis Methodology Application to Force Readiness Reporting. Reference (c) provides CJCS guidance for assessing the readiness of the Joint Force to execute assigned missions.

a. Relationship Between Readiness and Risk. Readiness and risk are distinct but interrelated concepts that share a foundation in capacity and capability.

(1) Readiness is assessed using resource metrics that measure personnel, equipment, maintenance, and training levels, as well as mission-essential task ratings, to evaluate capability. These assessments provide a comprehensive view of the Joint Force's ability to meet mission requirements.

(2) Risk, on the other hand, is evaluated through the lens of its nature, consequence, magnitude, and probability. Commanders use the Military Risk Matrix (Figure 28) and risk assessment methodology to identify risks to mission accomplishment and risks to force, framed in terms of impacts to capability and capacity.

b. Shared Metrics and Decision-Making. The relationship between readiness and risk is reflected in their shared metrics. Readiness evaluations inform risk assessments by identifying capability and capacity shortfalls, which contribute to both RM and RF. Commanders' assessments, including applied mitigations, provide critical inputs to the CJCS and Joint Staff for decision-making. These assessments enable leadership to make informed recommendations to SecWar regarding readiness and risk trade-offs in alignment with strategic guidance.

c. Maintaining Doctrinal Distinction. It is critical to recognize that readiness and risk are distinct doctrinal concepts: readiness must be assessed using standardized metrics for capacity and capability, while risk must be evaluated through the lens of probability and consequence. This distinction ensures that readiness reporting and risk assessments remain complementary but separate processes, each contributing to a holistic understanding of the Joint Force's ability to execute its missions.

4. Joint Risk Analysis Methodology Application from Intelligence Community Estimative Language. Reference (d) establishes IC analytic standards that govern the production and evaluation of analytic products. The following section establishes the methodology for integrating IC threat assessments into the JRAM. It provides the standardized crosswalk between the 7-level probability scale utilized by the JRAM.

a. Methodological Distinction. To accurately apply intelligence to operational risk, CCMDs and staffs must distinguish between the probability of a threat occurring and the probability of that threat causing mission harm.

(1) IC Threat Probability. Likelihood (probability) and confidence are distinct and independent elements of uncertainty that should not be placed in the same sentence. The IC assesses the probability of an adversary action or environmental event. Reference (d) requires analysts to characterize uncertainty associated with probability, utilizing an odd-numbered, 7-level scale that includes a neutral "Roughly Even Chance" (45–55 percent) median.

(2) JRAM Probability of Harm. As defined in Enclosure B, risk is the probability and consequence of an event or condition causing harm to a thing that is valued. The JRAM utilizes an even-numbered, 4-level scale (Very Unlikely, Unlikely, Likely, Very Likely) to promote a directional judgement on whether mission harm will occur, driving commander risk-mitigation decisions.

b. The Intelligence-to-Risk Translation Crosswalk. During the risk appraisal, assessors should utilize the crosswalk in Figure 19 to translate intelligence estimates into the JRAM probability baseline.

Crosswalk – Common IC Probability Expressions to JRAM Probability Scale	
Intelligence Community Directive (ICD) 203	JRAM Risk Plot
Almost certain(ly) / Nearly certain (95-99%)	Very Likely (~81-99%)
Very likely / Highly probable (80-95%)	
Likely / Probable (probably) (55-80%)	Likely (~51-80%)
Roughly even chance / Roughly even odds (45-55%)	*See Execution Paragraph (Boundary Flag)*
Unlikely / Improbable (improbably) (20-45%)	Unlikely (~21-50%)
Very unlikely / Highly improbable (05-20%)	Very Unlikely (~01-20%)
Almost no chance / Remote (01-05%)	

Figure 19. Intelligence-to-Risk Translation Crosswalk

c. IC Confidence. An element of uncertainty associated with probability, and required by reference (d), is confidence. Confidence is a factor of uncertainty and should be considered when assessing risk from adversary action. Confidence conveys the strength of evidence and argument supporting an assessment.

(1) High Confidence. Well-corroborated information from independent, proven sources; minimal contradictory reporting; low potential for deception; few information gaps. Strong and valid assumptions bridging information gaps; assumptions would not significantly affect the assessment if incorrect. Routine event that is well understood, relatively few variables.

(2) Moderate Confidence. Partially corroborated information from good sources; some potential for deception; several gaps. An assumption that changes the assessment if incorrect. Somewhat complex situation with multiple issues or actors; some previous examples that are well understood.

(3) Low Confidence. Uncorroborated information or low-confidence database records; high potential for deception; many critical gaps. More than one linchpin assumption with substantial effect on the assessment if incorrect. Highly complex or rapidly evolving situation with multiple issues or actors; few previous examples that are poorly understood.

d. Execution of the "Roughly Even Chance" Boundary. A fundamental principle of the JRAM is the prevention of neutrality when appraising risk. Therefore, an intelligence assessment of a "Roughly Even Chance" (45–55 percent) cannot be plotted as a neutral baseline.

(1) Mandatory Posture Assessment. When the IC provides a "Roughly Even Chance" assessment, it should trigger a mandatory handoff. The non-IC assessor should evaluate this ambiguous threat against force posture and existing mitigations.

(2) Forced Choice Plotting. Based on the posture assessment, the staffs will force the JRAM probability plot to either:

(a) Likely. If friendly forces are highly vulnerable, out of position, or lack rehearsed mitigations, the probability of the threat causing mission harm is assessed as Likely.

(b) Unlikely. If friendly forces are hardened, postured to react, or possess strong existing mitigations, the probability of the threat causing mission harm is assessed as Unlikely.

e. Documentation. When a "Roughly Even" intelligence assessment is translated to a JRAM plot of Likely or Unlikely, the staffs should document the specific friendly posture factors (vulnerabilities or mitigations) that drove the directional shift. This ensures decision-makers understand both the intelligence uncertainty and the operational judgement in the risk baseline.

5. Chairman's Risk Assessment

a. IAW reference (e), the CJCS must provide an annual risk assessment to SecWar and Congress about the MSR to national interests and MR to executing the NMS. The CJCS continually considers risk when fulfilling title 10 functions within the JSPS. Specifically, the CRA provides baseline risks that inform assessment and advisory actions throughout the year. The CRA cuts across processes and acts as a key feedback mechanism throughout the JSPS and for subsequent revisions to strategy. IAW reference (e), the CRA identifies and assesses changes in the strategic environment, threats, objectives, force planning and sizing constructs, and assumptions. It also addresses levels and categories of MSR to U.S. interests over time, military risks to execution of NMS objectives, and critical deficiencies and strengths in Joint Force capabilities, including key contributions from external support.

b. The Joint Staff develops the CRA using the JRAM described in Enclosure B. The **risk appraisal** portion of the framework is accomplished by the Joint Staff Directorate for Strategy, Plans, and Policy, J-5 with input from the CCMDs, Services, other Joint Staff elements, and the IC. IAW reference (e), if the CJCS characterizes a baseline risk as *Significant* or higher, SecWar is required to submit to Congress a plan for mitigating those risks. This **risk management** portion of the framework is addressed through the SecWar's RMP. It identifies needed adjustments to authorities, policies, priorities, operations, activities, and/or investments for each baseline *Significant* or *High* MSR and/or MR. Figure 20 shows how the JRAM is applied to the CRA. The CRA articulates the risk details regarding executing the NMS with the Joint Force using this JRAM as the foundation of risk judgment and communication.

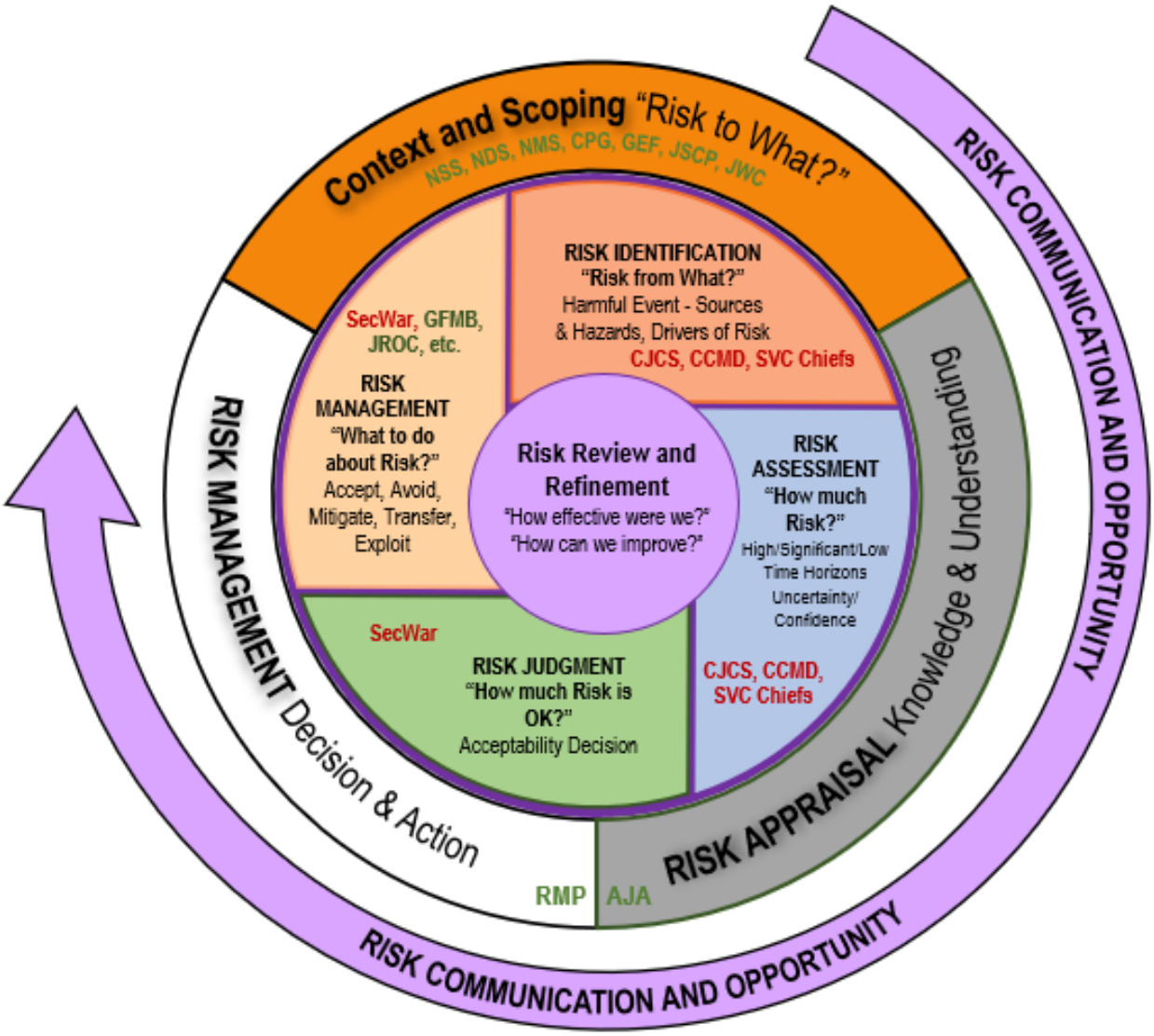


Figure 20. Joint Risk Analysis Methodology Framework Applied to the Chairman's Risk Assessment

6. Joint Risk Analysis Methodology Application to the Chairman's Risk Assessment

a. Context and Scoping. The CRA must characterize MSRs and MRs as they relate to the objectives identified in national strategic guidance, primarily the *National Security Strategy* (NSS) and NMS, respectively. MSRs and MRs should not be considered entirely independent of one another. A single source of risk may impact both strategy and military operations, while decisions to mitigate one type of risk may have a positive or negative impact on the other. Throughout the development of the CRA, the Joint Staff J-5 applies the JRAM as outlined in Enclosure B.

b. Risk Appraisal Process. The CRA is prepared by the Joint Staff J-5 using standardized definitions, probability, and consequence levels for each type of risk (Enclosure B). The CRA leverages multiple perspectives to delineate the sources and drivers of risk over time and the Nation's vulnerability to those threats. These inputs provide a basis for initial estimates of probability and expected consequences and set the stage for risk characterization. Most feedback comes from JSPS processes and products, including the *Annual Joint Assessment* (AJA) survey, which leverages the perspectives of each CCDR and Service Chief. Other inputs include, but are not limited to, the *Joint Staff Intelligence Estimate*, *Joint Force Readiness Review*, Forces For Unified Command Memorandum, Directed Readiness Tables, Availability Tables, *Cumulative Impacts to Strategic Readiness*, *Global Force Management Allocation Plan*, *Strategic Readiness Assessment*, *Semiannual Readiness Report to Congress*, and *Defense Planning Guidance* (DPG). The CRA considers risk across three time-horizons: near-term (0–3 years), mid-term (2–7 years), and long-term (5–15 years), which represents the combination of forces development and design.

(1) Military Strategic Risk. MSR is defined as **the probability and consequence of events, with direct military linkages, causing harm to U.S. national interests as defined in national strategic guidance**. These events—often stemming from strategic threats—create forces that can cascade across multiple regions and domains and may produce systemic impacts on homeland defense, alliances, strategic deterrence, and economic security, among others. MSR also represents the potential for compounding effects that fundamentally alter the strategic environment.

(a) Military Strategic Risk Assessment Framework. MSR has four probability levels and four consequence levels, depicted in Figure 21. As noted in the definition of MSR, the consequences are all tied to national interests. These interests are articulated in strategic guidance—primarily the NSS, NMS, and NDS, among others. The CJCS uses these interests as a starting point for assessment of MSR.

Probability of Event (P)
Very Likely (~81-99%)
Likely (~51-80%)
Unlikely (~21-50%)
Very Unlikely (~01-20%)

Consequence of Event (C) to US National Interests	
Extreme:	Existential/Permanent damage
Major:	Catastrophic damage
Modest:	Considerable damage
Minor:	Confined damage

Figure 21. Military Strategic Risk Probability and Consequence Levels

(b) Consequence Assessment and Strategic Value. The strategic value of the interest being examined must be considered when determining the consequence level. It is critical that strategic values or interests not become a function of a particular threat, but rather of what could suffer the risk of a harmful event. A threat assessment should not begin before considering national interests and their relative importance (the strategic thing of value). Doing so risks reacting to a threat with major commitments and resources devoid of any rational linkage to the relative value of critical interests. For example, the effect on U.S. national interests from a ballistic missile hazard varies depending on whether it is directed at the homeland, a treaty ally, or a partner. Thus, strategic value becomes part of determining whether a consequence is assessed as Minor, Modest, Major, or Extreme. To assist with this determination, Figure 22 frames the interest threatened and the degree of damage to that interest if a particular event were to occur. Note this list cannot account for all potential events.

	Harmful Event: Varying Degrees of Damage **Based on inherent damage to interest, time, and resiliency**			
National Interest "Risk to What?"	**Confined** **Near-term**	**Considerable** **Mid-term**	**Catastrophic** **Long-term**	**Existential** **Permanent**
Security of the American people	Small scale contingency ops (e.g. NEO, HA/DR) Tactical terror attack (Lone Wolf) Minor domestic civil disturbance American hostage(s) held Loss of access Cooperative security activity or arrangement canceled	Minor armed conflict Operational terror attack Isolated or minor attack on global domain or critical infrastructure Major domestic civil disturbance Isolated attack on U.S. embassy or business Loss of ally or partner Rise of regional hegemon Unsecured global domains Isolated epidemic or natural disaster	Theater war or major armed conflict Strategic terror attack Strategic attack on global domain / critical infrastructure Widespread major domestic civil disturbances Integrated regional attacks on U.S. embassies or business Invasion or loss of major ally or partner Regional security org. breakup Major epidemic or natural disaster	Nuclear war CBRNE terror attack Domestic rebellion Pandemic or natural disaster threatening U.S. existence
Economic prosperity and opportunity	Limited trade, resource, or financial interruption Confined interference in critical infrastructure Change in currency standard Minor cyber compromise	Extended trade, resource, or financial interruption U.S. recession Extended interference in critical infrastructure Failure of IMF Lack of international norms U.S. Depression	Financial failure of major institutions or markets Major degradation of critical infrastructure Access to global domain(s) disrupted by adversary	Global or U.S. economic collapse Close economic system Destruction of critical infrastructure Seizure of U.S. industry Access to global domain(s) denied by adversary
Deterrence of Military Threats	Minor gaps in readiness and force generation. Acute regional conflict drawing on U.S. force posture. Minor lapse in appropriations. Proxy-attack on U.S. asset. Minor treaty violation by U.S. ally.	Major gaps in readiness and force generation. Long-term conflict drawing on U.S. force posture and generation. Major lapses in appropriations. Collapse of regional alliance. Technological surprise.	Geographically selective ability to field a forward deterrent presence and posture. Inability to fund force modernization. Invasion of treaty ally.	Complete inability to field a forward deterrent presence and posture. Major re-alignment of global military alliances. Complete inability of the U.S. military to project power globally. Collapse of the Defense Industrial Base.

Figure 22. Military Strategic Risk Matrix – Consequence Development

(c) Determining Consequence Levels. Once an assessor has determined the degree of damage (confined, considerable, catastrophic, or existential) using Figure 22, a consequence level can be obtained using Figure 23 based upon the scale or scope of the strategic value of the interest. This consequence will be paired with probability over a time horizon to assess risk level during risk judgment. Risk assessments provided by CCMDs and Services are critical inputs to the CJCS in determining the risks articulated in the CRA.

	Harmful Event: Varying Degrees of Damage			
Strategic Value of Interest Scale / Scope	**Confined**	**Considerable**	**Catastrophic**	**Existential**
Homeland / Vital	**Modest**	**Major**	**Extreme**	**Extreme**
Ally / Global	**Modest**	**Major**	**Major**	**Extreme**
Partner / Regional	**Minor**	**Modest**	**Major**	**Major**
Other / Local	**Minor**	**Minor**	**Modest**	**Modest**

Figure 23. Military Strategic Risk Matrix – Consequence Assessment

(2) Military Risk. MR is defined as **the probability and consequence of events causing harm to the Joint Force's ability to execute assigned objectives**. This encompasses both internal and external forces that manifest as threats to military effectiveness across personnel, equipment, training, and operations. It involves orchestrating the performance of missions assigned by the President and SecWar with the military departments force design and force structure plans to meet the CCMDs' title 10 responsibilities. MR assessments must consider the Services' and force providers' total force (active, reserve, civilian, and contractor). There are two categories of MR: RM and RF. Both must be considered when calculating MR.

(a) Risk-to-Mission. RM is **the probability and consequence of planned and contingency events causing harm to current or future military objectives**.

1. Operational Risk. **The probability and consequence of failure to achieve mission objectives while protecting the force from unacceptable losses**. This risk subset considers the ability to execute current, planned, and contingency operations in the near-term time horizon. Commanders consider the feasibility of these plans in conjunction with operational concerns, such as the potential for escalation, to assess risk from a threat or hazard adequately. Decision-makers aggregate the Joint Force's ability to achieve mission objectives to measure the overall achievability of higher-level

military objectives called for by the current NMS within acceptable human, materiel, and financial costs.

2. Projected Mission Risk. **The probability and consequence of an anticipated event that may cause failure to meet projected operational mission requirements**. It reflects the future force's ability to achieve future mission objectives in the mid- and long-term time horizons and considers the future force's capabilities and capacity to deter or defeat emerging or anticipated threats. Investment or divestment of resources in current or future force mission requirements may increase current risk in favor of decreased projected mission risk. Leaders must consider the risk managed in the near term versus the mid- or long term in decision-making. Projected mission risk (military RM across the 2–15-year time horizon) should not be confused with the "long-term" time horizon (5–15 years) when considering the future environment.

Example: Projected Mission Risk

A notional adversary is developing and fielding advanced Integrated Air Defense Systems, long-range area denial weapons, and extreme range air-to-air capabilities that are expected to be fully operational in 7–10 years. This advancement, if realized, would significantly challenge the Joint Force's ability to achieve air superiority mission requirements in a future conflict.

Figure 24. Projected Mission Risk

(b) Risk-to-Force. RF is **the probability and consequence of planned and contingency events causing harm to the provisions and sustainment of sufficient military resources**.

1. Force Management Risk. Force Management Risk is **the probability and consequence of not maintaining the appropriate force size and structure ("breaking the force"), CCMD mission load and battlespace, force distribution among CCMDs, and global force disposition**. It reflects a force provider's ability to generate ready forces within capacities to meet current campaign and contingency mission requirements. This risk subset considers the ability to execute plans today for contingency missions (e.g., potential conflict arising over an economic exclusion zone or a disputed territory) over the near- and mid-term time horizons. Force management risk must also consider the challenges of strategic continuity and the choices that need to be made to balance operational requirements for campaigns and modernization requirements to build warfighting advantage.

2. Institutional Risk

(a) Institutional Risk is **the probability and consequence of the DoW failing to perform established functions**. It reflects the ability of organization, command, management, and force development processes and critical military and non-military infrastructure to plan for, enable, and improve national defense. It considers organization and process effectiveness, including the acquisition process, budgetary impacts, program health, the defense industrial base, and overall health of the force. The time horizon associated with institutional risk is much broader. All three time horizons impact institutional risk.

Example: Military Strategic Risk v. Military Risk

A threat of forces closing shipping lanes in an international strait presents MSR, as it threatens freedom of navigation and thus U.S. economic security. This poses a risk—with direct military linkages—to U.S. strategic interests.

The ability of the Joint Force to prevent closure of this strait, or force its re-opening, presents MRs.

In this way, we see that MSR and MR are not always entirely independent in nature, and can carry implications for the other.

Figure 25. Military Strategic Risk versus Military Risk

(b) MR is assessed using the four probability levels and four consequence levels depicted in Figure 26. As with MSR, judgment is required to integrate different levels of probability and consequence during risk assessment.

Probability of Event (P)
Very Likely (~81-99%)
Likely (~51-80%)
Unlikely (~21-50%)
Very Unlikely (~01-20%)

Consequence of Event (C) to NMS	
Extreme	• RM, Mission Failure, Objectives Unachievable • RF, No Sourcing Solutions Exist for Critical Requirements
Major	• RM, Objectives Minimally Achieved (consider time, priority) • RF, Shortfalls Exist for Critical Requirements
Modest	• RM, Objectives Mostly Achieved (consider time, priority) • RF, Worldwide Sourcing Solution Exist for Most Requirements
Minor	• RM, Mission Success, Objectives Achievable • RF, Joint Force Fully Sustained and Requirements Sourced

Figure 26. Military Risk Probability and Consequence Levels

(3) Future Military Risk

(a) Future Military Risk is **the estimated probability and consequence, looking 2–15 years into the future, that considers both RM**

(Projected Mission Risk) and RF (Institutional Risk). Future MR combines the probability and consequence of the risk to the future Joint Force's projected ability to achieve mission objectives and a projection of the future Joint Force's design. The latter considers projected acquisition processes and budgetary impacts as well as health of the force and the Defense Industrial Base.

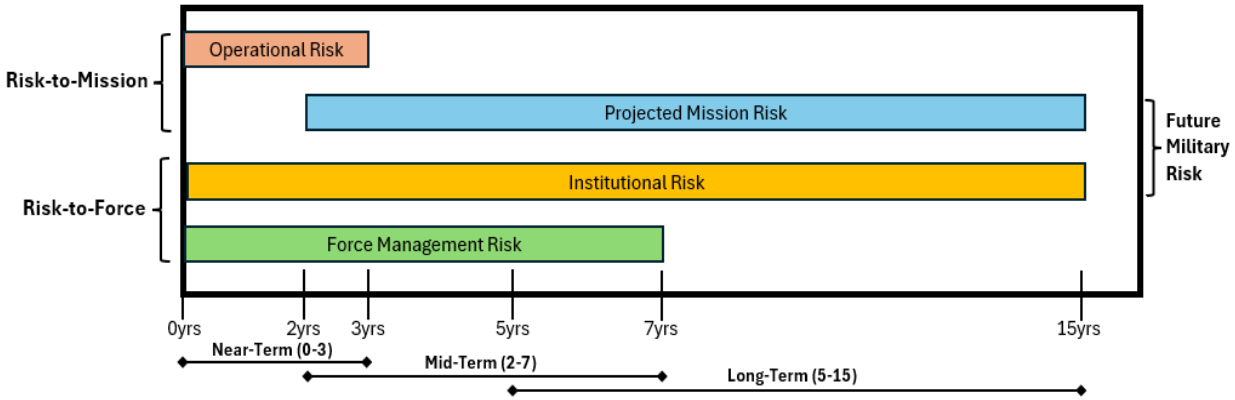


Figure 27. Military Risk Subsets Over Time Horizons

(b) The concepts of RM and RF can be differentiated into four total risk subsets (two each) based on source of risk and time horizon. Operational Risk and Projected Mission Risk relate to RM, while force management risk and institutional risk relate to RF. The time horizons presented are approximations and will remain subjective based on strategic trends, threats, and guidance provided by the CJCS and policy when informed by Risk-to-Strategy.

(4) Military Risk Consequence Assessment Matrix. Adopting the risk identification and assessment pillars (Pillars 1 and 2) from the methodology, assessors across the Joint Force use the Military Risk Consequence Assessment Matrix in Figure 28, in addition to the JRAM probability levels, to help frame the discussion on risk. In Figure 28, each row presents a risk subset or thing of value for consideration, with graduated consequences toward success or failure. After considering each applicable driver and assigning an expected result within the matrix, the assessor must use judgment to determine the overall expected consequence level for a situation. This tool provides a picture of MR consequences using common metrics for the Joint Force. However, the risk analysis is not limited to the metrics shown in Figure 28. CCMDs, Services, and other force providers should also consider Service red lines and any other metrics or analysis that facilitate a thorough assessment and enable communicating the risks.

Military Risk Subset	Reference	Risks to What	Minor	Modest	Major	Extreme
Current Mission / Force	UCP CPG EXORD	Achieve Objectives (CCMD Daily Ops)	Can fully achieve all OBJs (minimal costs)	Can achieve all critical OBJs (acceptable costs)	Can achieve only most critical OBJs (substantial costs)	Potential failure; can't achieve critical OBJs (unacceptable costs)
	GFM Assignment/Allocation	Meet CCDR Requirements (CCMD Daily Ops)	GFM sources ≥ 90% (some shortfalls)	GFM sources ≥ 80% (no critical shortfalls)	GFM sources ≥ 70% (critical shortfalls)	GFM sources < 70% (shortfalls cause mission failure)
Current & Future Mission / Force	CPG JSCP PLANORDs	Achieve Plan Objectives	As planned (minimal costs)	Limited delays (acceptable costs)	Extended delays (substantial costs)	Extreme delays (unacceptable costs)
	CRS / Plan Assessment (Contingency Sourcing)	Meet CCDR Requirements	Capacity to source plan requirements to achieve objective(s)	Shortfalls cause minor plan deviations (no critical shortfalls)	Shortfalls cause major plan deviations	Shortfalls cause plan failure
	CCMD	Authorities	Full authority provided to achieve all objectives	Sufficient authority provided to achieve most objectives, no critical shortfalls	Insufficient authority provided to achieve some critical objectives	Insufficient authority for key objectives, potential mission failure
	Plan Assessment	Resources Meet Required Timelines	As planned (minimal costs)	Limited delays (acceptable costs)	Extended delays (substantial costs)	Extreme delays (unacceptable costs)
	CCMD & Service	Partnerships	Partnerships effective	Critical partnerships effective	Critical partnerships partially effective	Critical partnerships ineffective, potential mission failure
		Messaging	Messaging effective	Key messaging effective	Key messaging partially effective	Key messaging ineffective, potential mission failure
		Capability: DOTMLPF-P vs Threat	Dominance	Superiority	Parity	Inferiority
	JFRR & DRRS	Readiness (DRRS)	Full spectrum C1 full capability	Ready for MCO C1/C2 some capacity shortfalls	Ready for minor armed conflict critical capabilities C1/C2 limited capacity	Critical capabilities < C2 capacity shortfalls cause mission failure
Future Mission / Force	GFM Allocation ** "Greater" being defined by the denominator (dwell) increasing relative to the numerator (deployment or mobilization).*	Stress on AC Force (D2D) DTM 21-005	D2D 1:3 or greater*	1:3 > D2D ≥ 1:2.5	1:2.5 > D2D ≥ 1:2	D2D threshold is 1:2
		Stress on RC Force (M2D) DoDI 1235.12	M2D 1:5 or greater*	1:5 > M2D ≥ 1:45	1:45 > M2D ≥ 1:4	M2D threshold is 1:4
		Stress on AC Mobility Force (T2D)	T2D > 1:2.5	1:2.5 > T2D > 1:2	1:2 > T2D ≥ 1:1.5	T2D < 1:1.5
		Stress on RC Mobility Air Force (T2D)	T2D > 1:5	1:5 > T2D > 1:4	1:4 > T2D ≥ 1:3	T2D < 1:3
		Modernization / Critical Maintenance	As planned (minimal costs)	Limited delays (acceptable costs)	Extended delays (substantial costs)	Extreme delays (unacceptable costs)
	RRAB/ JFRP / CPR	Programmatic	Meets or exceeds schedule, IOC or FOC; incurred savings	Minor delays milestone ≥ B; minor budget difficulty	Major delays milestone ≥ A; over budget (Nunn-Mcurdy)	Program failure; zeroed out (de-funded)
	RRAB/ JFRP / AJA	Force Development & Design Defense Industrial Base	Meets all mission requirements	Meet priority mission requirements (no critical shortfalls)	Critical shortfalls cause major plan deviations	Failure to meet essential requirements causes mission failure
	JWC JCC	Operational Imperatives & CRCs	Achieves all operational imperatives (no capability gaps)	Achieves priority operational imperatives (no critical capability gaps)	Achieves minimal operational imperatives (minor critical capability gaps)	Operational imperatives not achieved (major critical capability gaps)

Figure 28. Military Risk Consequence Assessment Matrix

c. CRA Risk Judgment

(1) CRA Risk Characterization. After evaluating the probability and consequence of sources and drivers of MSR and MR, events are assigned a risk level of *Low*, *Moderate*, *Significant*, or *High*. Risk can additionally be modified with Trending Up or Trending Down modifiers based on an assessed direction

of risk over a specific time horizon. Ultimately, the CJCS makes the final decision on risk levels conveyed in the CRA.

(2) Finalization and Submission. Once all MSRs and MRs have been characterized and approved by the CJCS, the Joint Staff J-5 finalizes the CRA and forwards it to the CJCS for signature. The CJCS then forwards the CRA to SecWar to evaluate and manage the risk. A visual representation of a final, integrated risk contour plot is exemplified in Figure 29.

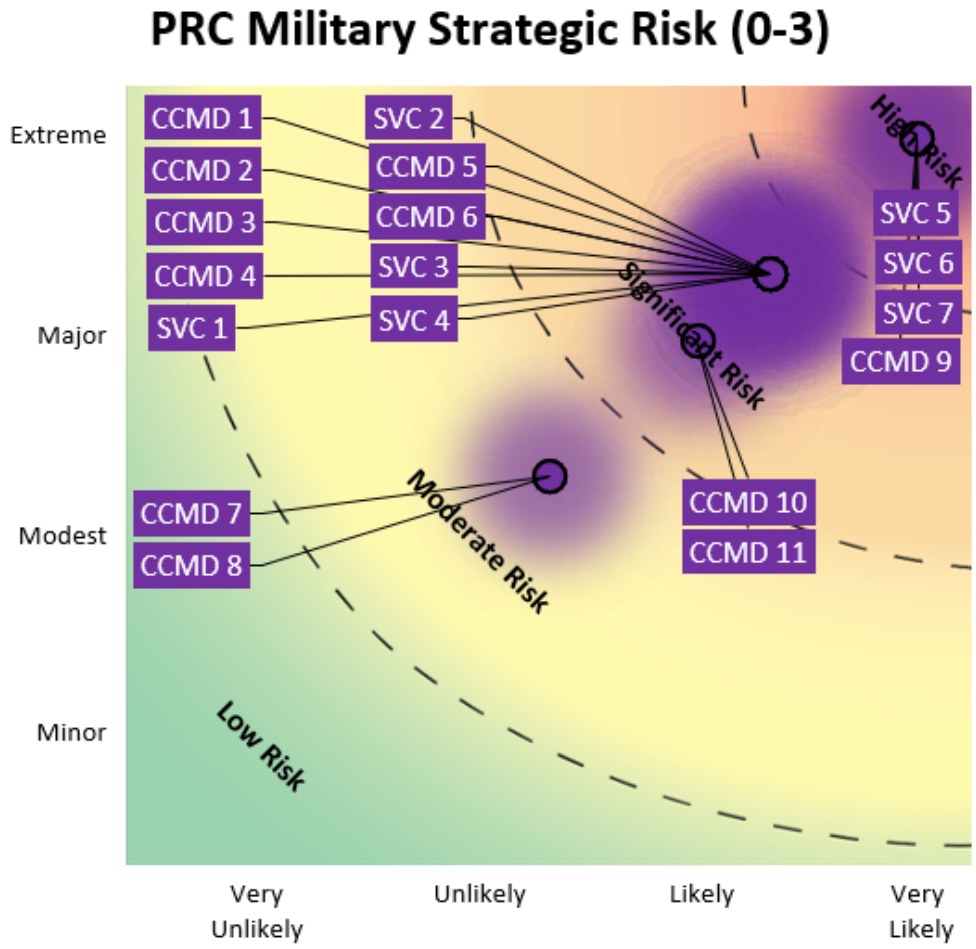


Figure 29. Example Combatant Command/Service Military Strategic Risk

(3) Strategic Feedback Function. The CRA serves as a critical feedback loop for the NMS in determining the ways and means required to accomplish the strategy. The CRA is also the impetus for an NMS revision should the assessment find that the strategic environment has changed and the level of risk becomes unacceptable.

d. CRA Risk Evaluation

(1) Risk Management and Decision Authority. SecWar determines the acceptability of risk presented in the CRA and develops options for managing the risk, which feed into the annual DPG. Depending on the situation, the SecWar may decide to accept, avoid, mitigate, or transfer the risk as described in Enclosure B. For example, the SecWar may mitigate risk in the near term by focusing resources on current issues and opportunities, while transferring risk to the mid-term or long term. In this case, if SecWar decides to transfer risk, the decision will need to be presented to the next highest authority, the President, for approval.

(2) Military Strategic Risk and Military Risk Trade-offs. Another major consideration during risk evaluation is to trade space between MSR and MR. Decision-makers must contemplate second- and third-order effects of risk decisions, as decisions made to manage MR have the potential to increase MSR. This trade-off can be represented on multiple layered, 2D risk contour charts, or represented across an anticipated timeframe as shown in Figure 30. This graphic does not represent a **comparison** between MSR and MR, but rather conveys how a single decision may impact both categories of risk.

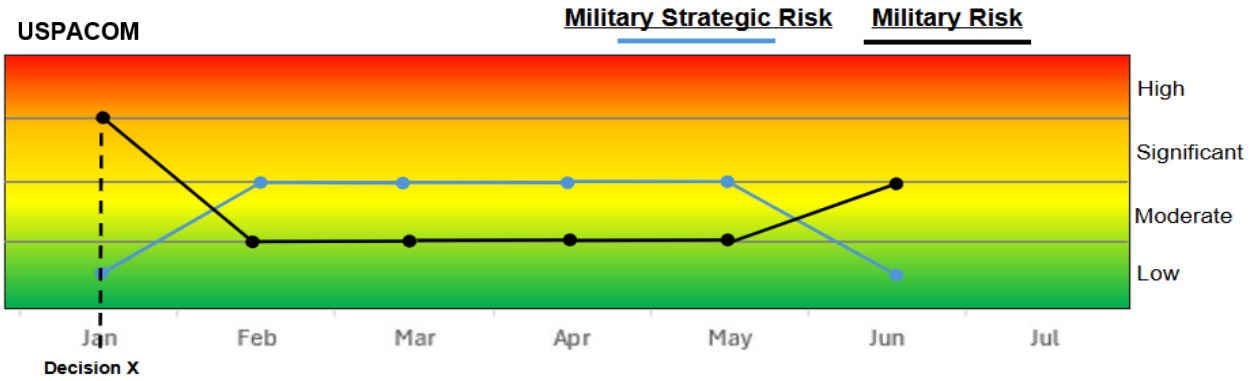


Figure 30. Example Military Strategic Risk/Military Risk Tradeoff Across Time

Chairman's Risk Assessment: Global Integration of Risk

The assessed MSRs and MRs from the CCDRs and Service Chiefs, provided within the AJA survey, are aggregated by the Joint Staff J-5 to formulate risk levels that encompass the CJCS's global view. The risk levels are calculated by leveraging the roles and responsibilities defined within the current Unified Command Plan to apply weighted, median values that relate to the trans-regional responsibility or physical area of responsibility origin of the threat or hazard examined. The CJCS convenes a Tank with the CCDRs and Service Chiefs to adjudicate risk levels from the derived aggregation to provide a globally integrated risk assessment, which SecWar delivers to Congress with an accompanying mitigation plan.

Figure 31. Chairman's Risk Assessment – Global Integration of Risk

(3) Comparative Risk Analysis. Comparison of disparate risk decision outcomes can and should be considered when making current decisions that may impact the future risk environment. This can reach across risk types, geography, and time horizons, where quick wins in one place and time should be analyzed for impact on strategy across other times and locations. For example, the choice to expend critical munitions now in one area may have implications for execution of military or military strategic objectives in another area in the future. This example is displayed in Figure 32, where munition expenditure in CCMD 1 lowers near-term MR while increasing risk in CCMD 2 across the near- and mid-terms as the expended munitions are expected to be replenished.

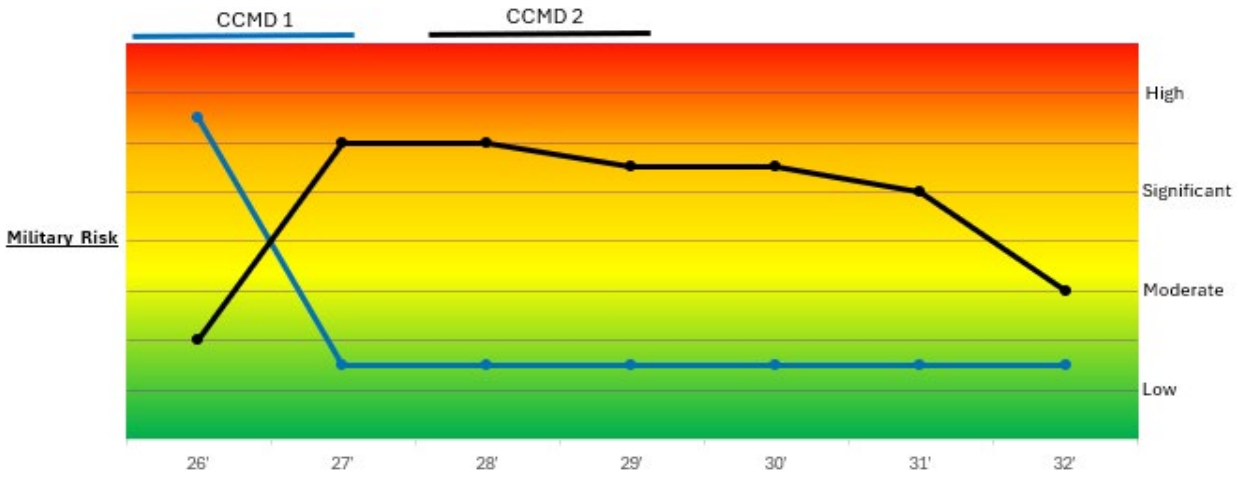


Figure 32. Comparative Risk Example – Military Risk Tradeoff Across Time

e. CRA Risk Management. The RMP is the formal means for SecWar to explain how the DoW will mitigate *Significant* or *High* risk identified by the CJCS. It is designed to address risk enterprise-wide and is normally developed in concert with the Joint Staff, CCMDs, and Services. The DoW mitigates risk

in many ways. MSR is mitigated by adjusting authorities, policies, budget, and priorities. The previously defined MR subsets—RM and RF (based on source and time horizon)—help determine the most effective ways to address that type of risk.

f. CRA Risk Communication. Clear communication between all leaders and staff is critical to achieving a cohesive and balanced CRA. For example, CCDRs and Service Chiefs must have a common understanding of terms, definitions, and how risk is characterized. This is necessary to properly convey risk in their AJA survey responses, which provide substantial inputs to the CRA. The Joint Staff and other contributors must have the same baseline understanding to ensure their feedback is relevant and appropriately aligned.

g. CRA Risk Trends. Historical context is an important consideration for senior leaders to fully understand the scope of the strategic environment when assessing risk and making risk decisions. This also applies to the CRA in how measured risks have evolved (or trended) over time. Figure 33 shows an example of historically plotted CRA risk ratings as they compare to the notional snapshot example given in Figure 29. It is important to remember that, while a variety of inputs affect the assessment of risk in the CRA, the ultimate determination of a CRA risk rating is at the discretion of the CJCS.

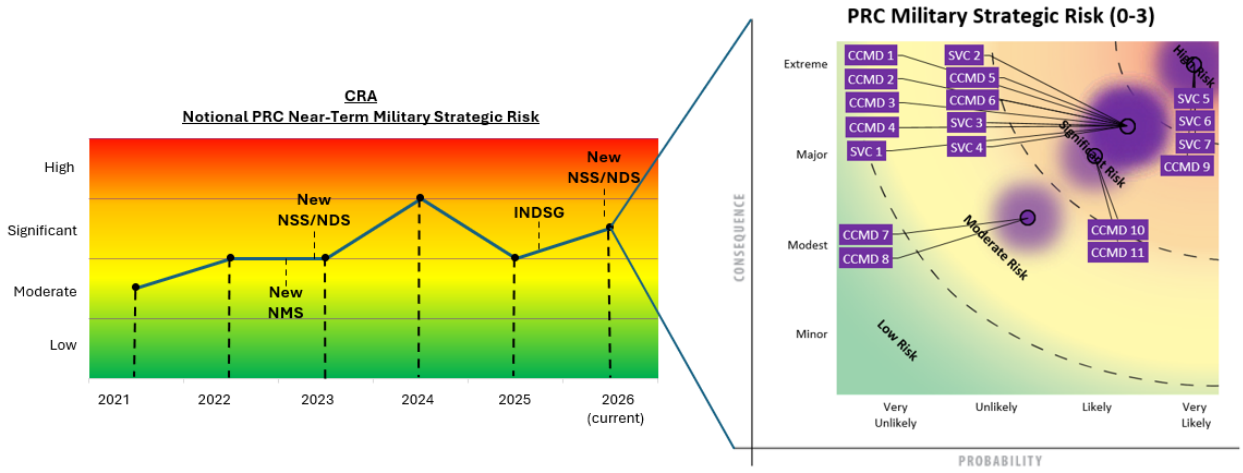


Figure 33. Risk Trends Example – Notional CRA Across Time

7. Summary. Strategic assessments serve as the keystone for risk calculations to the Nation's strategy and the Joint Force. The Joint Force will use Risk-to-Strategy as a tool to understand the strategic environment and to provide strategic assessments informing senior leader decision-making to set the conditions to deter or, if necessary, prevail in conflict.

ENCLOSURE D

RISK DOCUMENTS

1. Introduction. Practitioners study risk for various reasons. The study of risk crosses disciplines, from business and economics to science and technology, and is applicable to the military. The methodology and concepts presented in this manual are based on and aligned with the research accomplished across the broader risk community.

2. Joint Publications and CJCS Directives

a. Joint Publication (JP) 5-0, *Joint Planning*, discusses risk as part of planning and operations. JP 5-0 emphasizes the importance of risk identification and mitigation throughout the planning process. Risk in this context is focused on mission accomplishment and impact to mission.

b. JP 3-0, *Joint Campaigns and Operations*, delves into risk management as a function of command and a key planning consideration. It depicts a very basic risk management process.

c. The *DoD Dictionary of Military and Associated Terms* includes standard definitions for risk terms utilized in this manual.

d. CJCS Instruction (CJCSI) 3100.01F, 29 January 2024, "Joint Strategic Planning System" (reference (a)) explains how the CJCS meets statutory responsibilities as directed by U.S. Code. The CRA is a key JSPS document directed by U.S. Code.

e. CJCSI 3141.01F, 31 January 2019, "Management and Review of Campaign and Contingency Plans" explains how CJCS provides for the preparation and review of contingency plans and provides advice on global integration.

f. CJCSI 3401.01E, current as of 19 May 2014, "Joint Combat Capability Assessment" establishes the Joint Combat Capability Assessment as the policy and process for reporting and assessing DoW readiness to execute the NMS.

g. CJCSI 3401.02B, current as of 17 July 2014, "Force Readiness Reporting" (reference (c)) explains force readiness reporting to the President and SecWar to meet assigned missions and goals.

h. CJCS Manual 3130.06E, 12 May 2026, "Global Force Management Allocation Policies and Procedures" (reference (b)) amplifies this manual and

the GFMIG on how to assess and articulate risks in the GFM allocation process.

3. Non-Governmental Sources of Risk Knowledge

a. Documents from the International Risk Governance Council (IRGC) were particularly informative in developing this manual. The IRGC is a science-based independent think tank. This non-profit organization's mission includes "developing concepts of risk governance, anticipating major risk issues, and providing risk governance policy advice for key decision makers." The IRGC white paper "Risk Governance: Towards an Integrative Approach," by Ortwin Renn and Peter Graham, provided key background and substantiated fundamental concepts used when producing this manual.

b. The International Organization for Standardization (ISO) is another non-governmental international organization and independent resource. ISO 31000:2009, "Risk Management – Principles and Guidelines," provides principles, a framework, and a process for managing risk.

4. Risk in Other U.S. Government Agencies. This list of resources is not exhaustive, but it gives a sense of how risk is applied in other agencies.

a. U.S. Department of Commerce. DAO 216-20, 14 October 2016, *Enterprise Risk Management*, helps the Department of Commerce identify, assess, and mitigate risks that could impact strategic goals, operational performance, and technological initiatives.

b. National Institute of Standards and Technology. NIST SP 800-37 Rev 2, December 2018, *Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy* provides a lifecycle-driven process to integrate security, privacy, and supply chain risk management into systems development and operational processes.

c. Office of Management and Budget. OMB Circular A-123, 10 March 2026, *Internal Control Systems*, establishes enterprise risk management approaches for internal controls in federal agencies.

d. Department of Homeland Security. The *DHS Risk Lexicon*, September 2010, is part of the Department of Homeland Security's efforts to establish a common framework for overall management and analysis of homeland security risk.

e. Central Intelligence Agency. *Measuring Risk to US Interests: A Framework for Risk Exposure and National Strategic Importance*, 9 March 2015.

f. Office of the Director of National Intelligence. ICD 203, 12 June 2023, "Analytic Standards," establishes analytic standards that govern the production and evaluation of analytic products in the IC.

5. Risk in the Department of War

a. Office of the Chief of Naval Operations Instruction 3500.39, 29 March 2018, "Operational Risk Management" outlines how commands identify hazards, assess severity and probability, and apply risk controls.

b. Marine Corps Order 5100.29, 8 February 2022, "The Marine Corps Safety Management System" integrates risk management, mishap prevention, and safety assurance into daily operations.

c. Department of the Army Pamphlet 385-30, 2 December 2014, "Risk Management" details how to evaluate risk severity and probability and provides guidelines for determining acceptable risk levels.

d. Air Force Instruction 90-802, 20 January 2026, "Risk Management" mandates a standard process to identify and mitigate hazards to enhance operational effectiveness, preserve resources, and protect personnel.

e. DoD Instruction (DoDI) 6055.01, 14 October 2014, "DoD Safety and Occupational Health (SOH) Program" provides overarching DoW guidance regarding risk principles and risk management with respect to health and safety. The instruction provides a five-step risk management process that is used across all Services to help ensure synergy across Joint Force operations. The risk management strategies are applied to eliminate occupational injury or illness and loss of mission capability. They are intended for use in all military operations and activities, including acquisition, procurement, logistics, and facility management.

f. Another DoW document, "Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs," June 2015, focuses on the relationship between effective risk management and programmatic success. It provides guidance on establishing a risk management program for defense acquisition programs.

g. DoDI 8510.01, 19 July 2022, “Risk Management Framework for DoD Information Technology,” describes policy and procedures applicable to the integrated enterprise-wide structure for cybersecurity risk management.

h. The DoW’s definition of GFM in the *Global Force Management Implementation Guidance* includes the proactive balancing of risk.

i. “Risk of Strategic Deterrence Failure” (RoSDF) is a globally integrated, strategic assessment U.S. Strategic Command produces for the DoW, in collaboration with interagency and ally partners, under its Unified Command Plan-assigned Strategic Deterrence planning mission. RoSDF assesses “the risk there will be a failure of deterrence that results in an attack or series of attacks, regardless of means, that causes or was intended to cause catastrophic or existential effects on U.S. vital interests that could drive consideration of a strategic response.” The assessments are aligned with DoW planning time horizons, and provide decision makers and planners with a global sight picture of strategic risk factors from across the diplomatic, informational, military, and economic spectrum, and their estimated impact on adversary decision-making.

j. “Risk of Nuclear Attack,” as a subset of RoSDF, addresses risk that the means of the referenced “attack or series of attacks” might be nuclear.

GLOSSARY

PART I – ABBREVIATIONS AND ACRONYMS

Items marked with an asterisk (*) *have definitions in PART II*

AJA	Annual Joint Assessment
C	Consequence
CCDR	Combatant Commander
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
COA	course of action
CRA	Chairman's Risk Assessment
DHS	Department of Homeland Security
DoDI	DoD Instruction
DoW	Department of War
DPG	Defense Planning Guidance
GFM	Global Force Management
GFMIG	Global Force Management Implementation Guidance
IAW	in accordance with
IC	Intelligence Community
IRGC	International Risk Governance Council
ISO	International Organization for Standardization
J-5	Joint Staff Directorate for Strategy, Plans, and Policy, J-5
JP	Joint Publication
JRAM*	Joint Risk Analysis Methodology
JSPS*	Joint Strategic Planning System
MR*	Military Risk
MSR*	Military Strategic Risk
NDS	National Defense Strategy
NIST	National Institute of Standards and Technology
NMS	National Military Strategy
NSS	National Security Strategy
OMB	Office of Management and Budget

P	Probability
RF*	Risk-to-Force
RM*	Risk-to-Mission
RMP	Risk Mitigation Plan
RoSDF	Risk of Strategic Deterrence Failure
SecWar	Secretary of War

PART II – DEFINITIONS

Unless otherwise sourced, terms are for this document only.

accumulated risk. Accounts for a macro view of the risk environment, to include past events and decisions that have impacted the current risk environment.

action. Decisions and measures taken by the Joint Force or other stakeholders that alter posture, plans, readiness, resources, concepts, or behavior in ways that affect risk.

Calculated Risk. The conscious acceptance of potential assessed negative impacts of a decision to seize initiative, gain advantage, or accomplish the mission

drivers of risk. Factors that influence the probability or consequence of risks arising from various sources.

Force Management Risk. The probability and consequence of not maintaining the appropriate force size and structure ("breaking the force"), Combatant Command (CCMD) mission load and battlespace, and global and CCMD force disposition.

Future Military Risk. The estimated probability and consequence, looking between 2 and 15 years into the future, that considers both Risk-to-Mission (Projected Mission Risk) and Risk-to-Force (Institutional Risk).

harmful event. A harmful event is a foreseeable occurrence or persistent condition that, if it happens, will negatively impact what is valued in the risk context statement.

hazard. Conditions—internal or external to the Department of War—that can enable or amplify harm or advantage.

inaction. The deliberate decision to not change posture, plans, readiness, resources, or other factors when such changes are feasible.

Institutional Risk. The probability and consequence of the Department of War failing to perform established functions.

Joint Risk Analysis Methodology. Consistent, standardized framework to appraise, manage, and communicate risk. Also called JRAM.

Joint Strategic Planning System. The primary means by which the Chairman of the Joint Chiefs of Staff fulfills statutory responsibilities under title 10, U.S. Code, maintains a global perspective, leverages strategic opportunities, translates strategy into outcomes, and develops military advice for the Secretary of War and the President. Also called JSPS.

Military Risk. The probability and consequence of events causing harm to the Joint Force's ability to execute strategic objectives. Also called MR.

Military Strategic Risk. The probability and consequence of events, with direct military linkages, causing harm to U.S. national interests as defined in national strategic guidance. Also called MSR.

Operational Risk. The probability and consequence of failure to achieve mission objectives while protecting the force from unacceptable losses.

Projected Mission Risk. The probability and consequence of an anticipated event that may cause failure to meet projected operational mission requirements.

Quantitative Risk Analysis. A data-driven approach that uses numerical and statistical models to assign a value to risk.

risk. The probability and consequence of an event or condition causing harm to a thing that is valued.

risk acceptance. An informed decision to act without conducting risk mitigation efforts.

Risk Appraisal. A component of the Joint Risk Analysis Methodology, during which knowledge and understanding is generated. This component is applied to the Chairman's Risk Assessment through the Annual Joint Assessment process.

Risk Assessment. Second pillar of the Joint Risk Analysis Methodology, where we answer the question "how much risk?". Characterize risks by assessing probability and consequence, taking time into account.

risk avoidance. Forgoing the activity that would produce unacceptable risk or remove the item of value that could be damaged due to unacceptable risk.

Risk Characterization. Sub-set of Risk Assessment (Pillar 2), during which events are assigned a level of risk.

Risk Communication. A component of the Joint Risk Analysis Methodology encompassing the exchange of risk perspectives across processes and among leadership, primarily using risk statements.

Risk Evaluation. Sub-set of Risk Judgment, during which a decision maker determines the acceptability of a risk.

Risk Exploitation. Consider the "upside" of risk by deliberately accepting or re-balancing risk to pursue opportunities that can create or enhance advantage.

Risk Identification. First pillar in the Joint Risk Analysis Methodology, where we answer the question "risk from what?". Harmful events are identified, and sources and drivers of risk mapped.

Risk Judgment. Third pillar in the Joint Risk Analysis Methodology. Qualitative process focused on determining the degree of acceptable risk, considering both action and inaction.

Risk Level. A function of probability and consequence classified as *Low*, *Moderate*, *Significant*, or *High*.

Risk Management (Pillar). The fourth pillar of the Joint Risk Analysis Methodology (JRAM), and a major component. In JRAM, it is where risk decisions to accept, avoid, mitigate, transfer, or exploit risk are designed, implemented, and monitored.

Risk Management (Component). As a component applied to the Chairman's Risk Assessment, this encapsulates the Secretary of War's corresponding Risk Mitigation Plan.

Risk Mitigation. An action that reduces the probability or consequence of harm.

Risk Opportunity. A function of the five pillars where tradeoff and/or management of risk creates opportunities to produce an advantage.

Risk Statement. A statement that clearly expresses probability, the harmful event, time horizon, key drivers, consequence, overall risk level and trend.

Risk-to-Force. The probability and consequence of planned and contingency events causing harm to the provision and sustainment of sufficient military resources. Also called RF.

Risk-to-Mission. The probability and consequence of planned and contingency events causing harm to current or future military objectives. Also called RM.

risk transfer. Taking action to change when and where the risk is incurred and potentially who or what incurs it.

sources of risk. Threats or hazards which, alone or combined, have potential to cause harm to the thing that is valued.

threat. State or non-state actors that possess the capability and intent, or potential intent, to affect what is valued, whether through military, informational, economic, cyber, or other means.

(INTENTIONALLY BLANK)
Inner Back Cover

INTENTIONALLY BLANK
(BACK COVER)