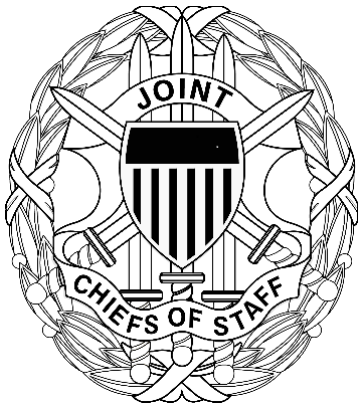


UNCLASSIFIED



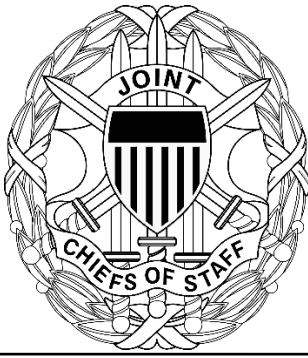
CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

JOINT RISK ANALYSIS METHODOLOGY

CJCSM 3105.01B

22 December 2023

UNCLASSIFIED



UNCLASSIFIED

CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-5

DISTRIBUTION: A, B, C

CJCSM 3105.01B

22 December 2023

JOINT RISK ANALYSIS METHODOLOGY

1. Purpose. This manual establishes the Joint Risk Analysis Methodology (JRAM) and provides guidance for appraising, managing, and communicating risk. It introduces and describes a common risk lexicon to facilitate consistency across Department of Defense (DoD) and Joint Force risk-related processes.

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, U.S. Code responsibilities, including the *National Military Strategy* (NMS) and *Chairman's Risk Assessment* (CRA). This manual places the CRA in context with 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 Superseded. CJCSM 3105.01A, 12 October 2021, "Joint Risk Analysis Methodology," is hereby superseded.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. Call-out boxes were added to enhance understanding with respect to definitions and examples. Enclosure C has been rearranged to align with and reflect strategic guidance direction to communicate Risk-to-Strategy through assessments. Various figures have been updated. Additional fidelity on the use and understanding of *Trending Up*

UNCLASSIFIED

UNCLASSIFIED

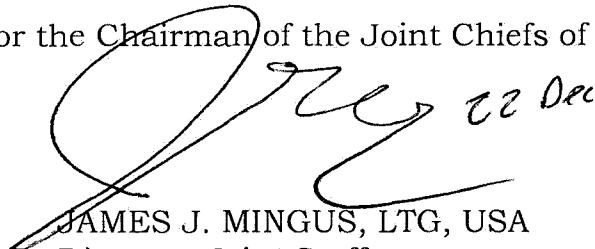
CJCSM 3105.01B
22 December 2023

and *Trending Down* risk statement modifier terms has been included. Greater emphasis has been put on the narrative around the communication of risk, and the global and temporal aspect of viewing risk as an opportunity. The glossary terms have been added and defined. Time horizons have been standardized to align with JSPS. The rest of the changes are administrative in nature.

6. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on the Non-classified internet Protocol Router Network. DoD Components (to include the CCMDs), other Federal agencies, and the public may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at: <<http://www.jcs.mil/library>>. Joint Staff activities may also obtain access via the SECRET Internet Protocol Router Network Directives electronic library web sites.

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

For the Chairman of the Joint Chiefs of Staff:



JAMES J. MINGUS, LTG, USA
Director, Joint Staff

Enclosures

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

UNCLASSIFIED

CJCSM 3105.01B
22 December 2023

TABLE OF CONTENTS

ENCLOSURE A – RISK AND THE JOINT FORCE.....	A-1
Introduction.....	A-1
JSPS and Risk	A-1
Summary.....	A-2
ENCLOSURE B – JOINT RISK ANALYSIS METHODOLOGY.....	B-1
Introduction.....	B-1
Framework.....	B-1
JRAM Application	B-2
Other Considerations	B-9
ENCLOSURE C – RISK-TO-STRATEGY – STRATEGIC ASSESSMENTS.....	C-1
Introduction.....	C-1
JRAM Application to Global Force Management.....	C-1
JRAM Application to Force Readiness Reporting.....	C-2
JRAM Application to the CRA.....	C-5
Summary.....	C-13
ENCLOSURE D – RISK REFERENCE DOCUMENTS.....	D-1
Introduction.....	D-1
Joint Publications and CJCS Directives.....	D-1
Non-Governmental Sources of Risk Knowledge.....	D-1
Risk in Other U.S. Government Agencies.....	D-2
Risk in the Department of Defense	D-2
GLOSSARY	GL-1
Part I – Abbreviations and Acronyms.....	GL-1
Part II – Definitions	GL-2

LIST OF FIGURES

1. Organizations and Risk	A-2
2. The Joint Risk Framework	B-2
3. Probability Levels	B-5
4. Consequence Levels	B-5
5. Baseline Risk Levels and Generic Risk Contour	B-6
6. Risk Across Strategic Continuum Time Horizons	B-11
7. Globally Integrated Approach to Risk	B-12
8. Globally Integrated Time Horizons	B-13
9. Military Risk Consequence Assessment Matrix	C-3
10. JRAM Applied to the CRA	C-5
11. Military Strategic Risk Probability and Consequence Levels	C-6
12. Military Strategic Risk Matrix – Consequence Development	C-7
13. Military Strategic Risk Matrix – Consequence Assessment	C-8
14. Military Risk Subsets over Time Horizons	C-9
15. Military Risk Probability and Consequence Levels	C-10
16. Example CCMD/Service Military Strategic Risk CRA Contour Plot	C-11

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 risk analysis comprehensively throughout the JSPS. In this methodology, commanders and staffs use a framework that appraises, manages, and communicates risk. This framework includes four pillars: problem framing, risk assessment, risk judgment, and risk management. The JRAM enhances risk communication and decision making by using the same terms and processes to communicate Military Strategic Risk (risk to national interests) and Military Risk (risk to executing the NMS, to include Risk-to-Mission and Risk-to-Force). The methodology described in this manual, coupled with military judgment, determines risk levels and mitigation strategies to facilitate risk-informed decisions. This methodology is meant to be structured to provide a common lexicon across the Joint Force community, yet flexible enough to be applied to a diverse set of risk assessment products.

2. Joint Strategic Planning System and Risk. Assessing risk throughout the JSPS provides the foundation for CJCS as the global integrator to fulfill title 10, U.S. Code responsibilities.

a. Commanders and 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 mitigation for Military Strategic Risk and Military Risk in a global strategic context.

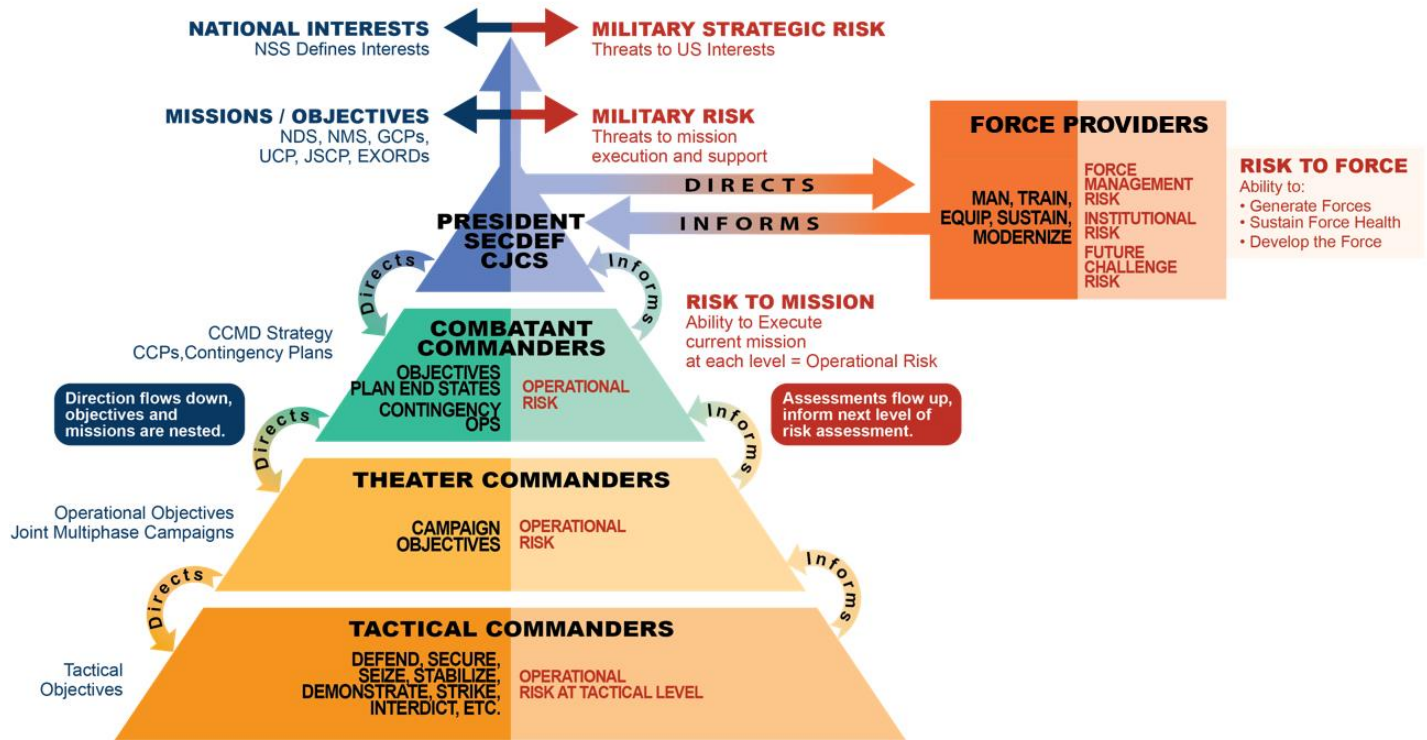


Figure 1. Organizations and Risk

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

ENCLOSURE B

JOINT RISK ANALYSIS METHODOLOGY

1. Introduction. Risk is the probability and consequence of an event causing harm to a thing that is valued. In many instances, the object(s) or item(s) of value is/are the objective(s) outlined in strategic guidance. Risk is assessed within one of four baseline risk levels (*Low, Moderate, Significant, or High*). It is at the discretion of the assessor to add modifiers to the baseline risk level, which will be addressed below. The JRAM provides a consistent, standardized framework to appraise, manage, and communicate risk at the appropriate level of responsibility, allowing leaders to make risk-informed decisions across disparate processes. Risk appraisal is fundamentally a qualitative process incorporating and informing commander's judgment while quantitatively expressing probability and consequence when appropriate. Risk, defined by probability and consequence, should be described within the applicable time horizon. However, the actual process of assessing risk is often a continuous one due to the dynamic nature of the strategic environment. As such, there may be times during this process that an assessor will need to reassess or re-characterize risk due to actions, reactions, or changes in the strategic environment. This framework is flexible enough that risk-related processes can adapt portions of it, but the foundation for risk assessment is built off the constant elements of probability, consequence, time, global integration, and risk level.

2. Framework. The JRAM framework consists of four major components (risk appraisal, risk management, risk communication, and risk opportunity), and four pillars to comprehensively address risk (Figure 2).

a. Pillars

(1) Problem Framing. Identifying the item, idea, or objective that is valued ("risk to what?").

(2) Risk Assessment. Identifying and scaling threats ("risk from what?").

(3) Risk Judgment. Developing a risk profile ("how much risk?") and evaluating the risk ("how much risk is ok?").

(4) Risk Management. Decisions and actions to accept, avoid, mitigate, or transfer risk ("what should be done or not done about the risk?").

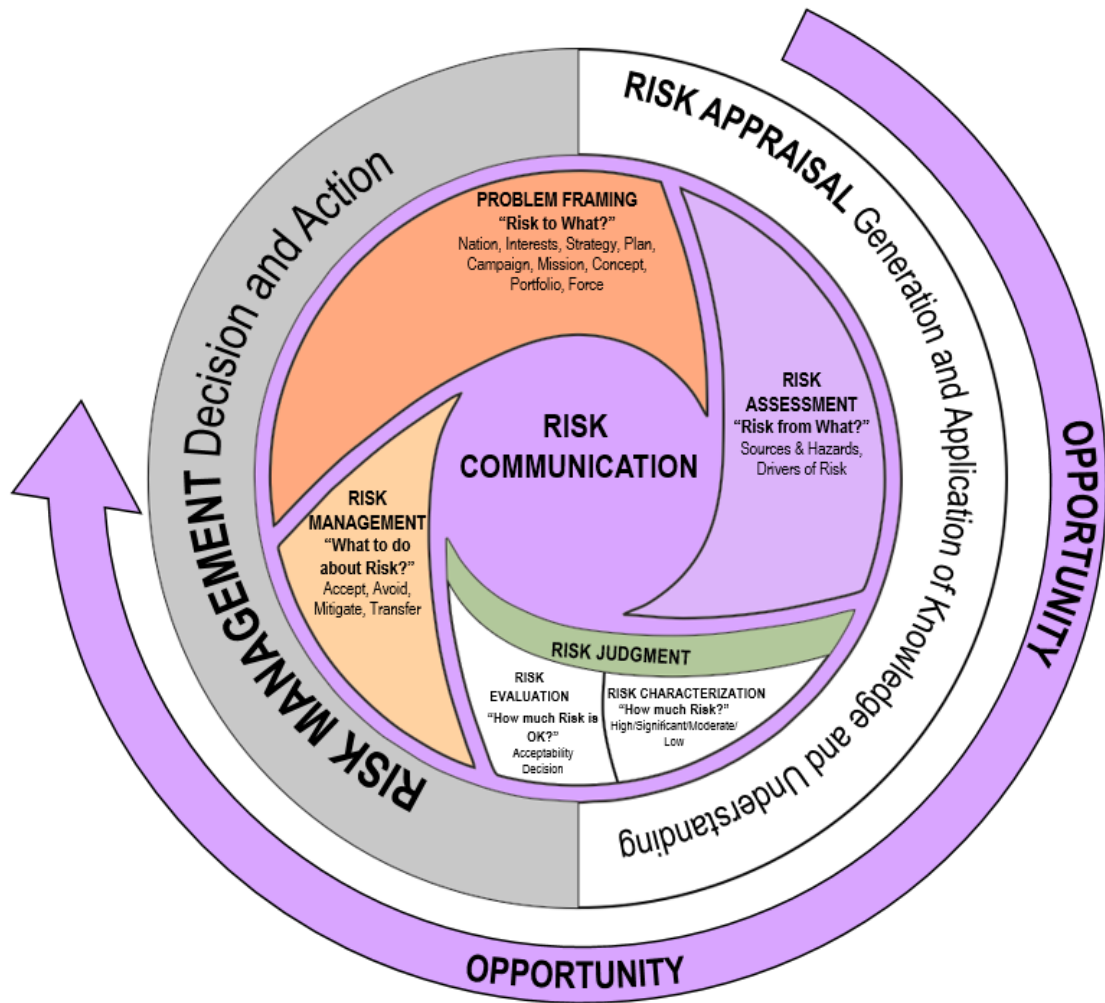


Figure 2. The Joint Risk Framework

3. JRAM Application

a. Problem Framing (Pillar 1). The first pillar of the JRAM is to frame the problem by identifying the item or idea—oftentimes an objective—that is valued and has the potential to be harmed. Protecting national interests, successfully executing a strategy or plan, or maintaining a viable, ready force are examples of relevant risk topics. To frame the problem, the assessor must answer the question “risk to what?” The assessor will coordinate with the risk owner, who is the individual ultimately responsible for appropriately managing a given risk (e.g. a Service Chief, a Combatant Commander (CCDR), a Secretary of a Military Department, of the Secretary of Defense (SecDef)). The assessor and the risk owner will define the standards (criteria, scale, terms, assumptions, etc.) to use and stakeholders to involve during the assessment. Problem framing must articulate strategic thinking across time to enable senior leaders to make risk decisions consistent with strategy. One example is the

three time horizons from the JSPS continuum of strategic direction: near-term (0–3 years), mid-term (2–7 years), and long-term (5–15 years). Strategic thoughts that do not consider time horizons undercut efforts to adapt and innovate the Joint Force for the necessary advantages against adversaries and make risk comparisons across commands, functions, and domains difficult. Problem framing must also consider the interdependent risks from CCMDs, Services, allies, partners, and non-military entities. In addition, problem framing should also consider a globally integrated perspective; for example, determining the possible ramifications of actions in one area of responsibility on other regions or domains. When appropriate, assessors may link multiple separate risks together to analyze how their aggregation can change the overall risk picture. Strategic thoughts that only focus on one of these perspectives leaves risk along the seams unexamined and fails to adopt an enterprise approach to the Joint Force increasing or decreasing risk in other areas.

b. Risk Assessment (Pillar 2). This pillar contains the following elements of effective risk assessment: harmful event, probability, and consequence. These three elements are essential to the understanding and communication of risk. The assessments of the harmful event (comprised of sources and drivers of risk), probability, and consequence should include a detailed analysis—quantifiable where possible—to support decision making in the risk judgment pillar. In order to understand a harmful event, the first step begins with identification of the source(s) and driver(s) of risk that may increase or decrease the probability or consequence. At any point during this process, the dynamic nature of the strategic environment may warrant a re-assessment and reconsideration of risk.

(1) Harmful Event. A foreseeable event in the future, singular or persistent, that harms the item or idea that is valued. It requires, at minimum, a source and driver of risk. For unforeseen events, or strategic deviations, refer to uncertainty.

(a) Sources of Risk. Threats or hazards that, alone or in combination, have the potential to harm the item or idea that is valued.

1. Threat. A state or non-state entity with the capability and intent to cause harm.

2. Hazard. Security, environmental, demographic, political, technical, or social conditions with potential to cause harm. Hazards can be either internal or external entities.

(b) Drivers of Risk. Factors that act to change the risk probability or consequence arising from various sources. They must be considered across

a specific time horizon, such as the three time horizons of near-term (0–3 years), mid-term (2–7 years), and long-term (5–15 years). Drivers can increase or decrease risk. A driver that may increase risk in one time horizon may become obsolete or reduce risk when considered in a future time horizon. Drivers shape the environment that enables or minimizes the harmful event. They may be both internal and external to an organization. Other risk driver considerations include, but are not limited to:

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

2. Vulnerability. The susceptibility of an asset, force, or mission to harm from a threat or hazard due to a weakness in security, design, or resilience characteristics.

3. Resilience. The ability to withstand, endure, and recover from disruption. In other words, how quickly the Joint Force can recuperate. 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.

4. Criticality. The importance or degree of dependency on the thing of value.

5. Accessibility. How easily a hostile force or capability can reach the thing of value.

6. Recognition. How easily the thing of value can be identified by a hostile force or capability, including its significance to the Joint Force.

7. Impact. How severe the damage is, including the secondary and tertiary effects of damage to the thing of value.

8. Resources. People, equipment, funding, locations, or ideas available to respond to a threat or hazard; that is, what we will use to mitigate the threat or hazard to reduce risk.

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

(2) Probability and Consequence. Once the assessor has identified the known sources and drivers of risk, they must determine the expected probability and consequence of the harmful event using the criteria established during problem framing. This includes defining the levels of probability and consequence, which should be standardized within a process by the risk owner.

Probability of Event (P)
Very Likely (~81-100%)
Likely (~51-80%)
Unlikely (~21-50%)
Very Unlikely (~0-20%)

Figure 3. Probability Levels

(a) Probability. Probability (P) is the determination of the likelihood, supported by confidence levels, of a harmful event occurring. To enable unambiguous risk communication, probability should be clearly and quantifiably defined. For this generic example, a four-level table helps the assessor designate level of probability of an event occurring (Figure 3). The levels “Very Likely” and “Very Unlikely” are assigned smaller ranges to ensure these two levels are reserved for events with a higher degree of certainty (i.e., more certain to happen or not to happen). The “Likely” and “Unlikely” levels capture the less certain outcomes. The definitional structure deliberately omits a level for very low, zero, or negligible probability. While pursuing a strategy and an associated force structure that operates without risk may be desirable, the cost of moving from “Very Unlikely” to zero probability may require an exponential increase in resources. Resources are finite—commanders and staff must spend time and energy efficiently through risk management. When determining a probability level, it is important to weigh all applicable drivers that may change the risk level. Furthermore, when appropriate, assessors may weigh confidence, which is an expression of the strength of information, the assumptions that underpin analysis, and the degree of gaps.

(b) Consequence. Consequence (C) is the impact or resulting harm if the event occurs and negatively impacts U.S. interests. Similar to probability, consequence should be clearly defined to ensure unambiguous risk communication. For this generic example, a four-level table helps the assessor designate level of consequence of an event occurring (Figure 4). These levels from “Extreme” to “Minor” should be tailored to describe specific risk scenarios. Harm is generally estimated considering vulnerability, resilience, criticality, impact, and resources. An example of “modest harm” would be the ability for the current mission/force to achieve all its critical objectives with acceptable costs, while “major harm” would be the

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 4. Consequence Levels

ability for a current mission/force to achieving only its most critical objectives with substantial costs (more granularity provided in Figure 15).

c. Risk Judgment (Pillar 3). Risk judgment is ultimately a qualitative effort aimed at determining a decision maker's degree of acceptable risk. It should be factually supported to enable an informed decision at the appropriate level of responsibility. It involves two actions—risk characterization and evaluation.

(1) Risk Characterization. Risk characterization establishes a risk level for each potential threat or hazard. The risk level is a function of the previously assessed probability and consequence. Plotting the probability and consequence on a risk contour graph can help determine an initial baseline risk level. This visual depiction of the assessed probability and consequence will allow subject matter experts or decision makers to determine an appropriate risk level. Figure 5 illustrates the baseline risk levels of *Low*, *Moderate*, *Significant*, and *High*, which should remain constant across Joint Force risk assessments.

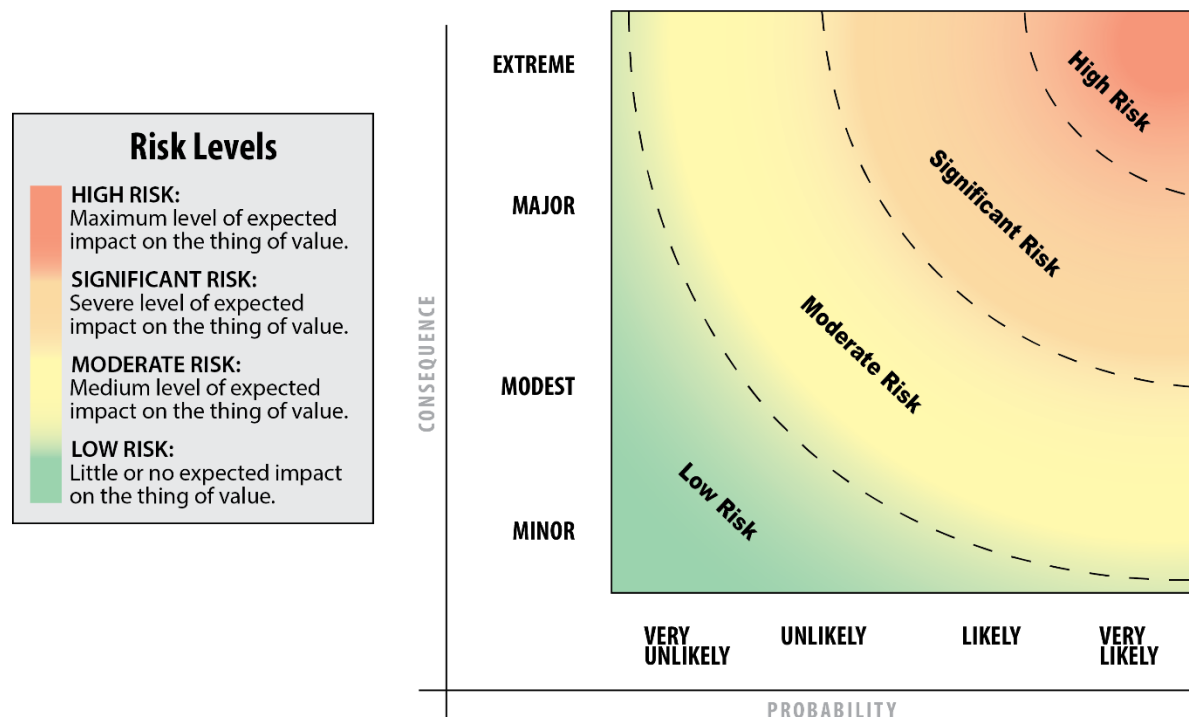


Figure 5. Baseline Risk Levels and Generic Risk Contour

Risk = Probability x Consequence

Adhering to the risk contour in Figure 5, a harmful event assessed with a “Very Likely” probability and “Minor” consequence is characterized as *Moderate* risk. Separately, a harmful event with “Very Unlikely” probability and “Extreme” consequence is also *Moderate* risk. While the risk levels are 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.

(2) Trending Modifiers. Risk levels can convey the temporal aspect by appending *Trending Up* or *Trending Down* modifiers to the baseline risk level. These modifiers reflect an assessed direction of risk across the specified time horizon if left unattended before risk management is applied, characterizing the intersection between the X- (Probability), Y- (Consequence), and Z-Axis (Time). This is particularly helpful when communicating a threat or hazard that exists over the time horizon assessed. For example, a risk characterized as *Significant Trending Up* across a 0–3 year time horizon indicates that the risk is *Significant* and has the potential to be *High* by the end of the third year. Note that *Low Trending Down* and *High Trending Up* are not qualifying risk levels due to *Low* and *High* being the bounding quantifiers within the scale. If, for example, an assessor determines that a *Moderate Trending Up* risk is becoming more likely or there is a higher consequence, the assessor should provide this detail either visually on a similar risk contour graph or with a built-out risk statement. Assessors should identify and analyze the expected impacts of risk drivers when considering modifiers.

(3) Risk Evaluation. During risk evaluation, a decision maker judges the acceptability of a risk, which will inform decisions on how to manage the risk. Risk evaluation gives decision makers the space to manage risk in an opportune way that in theory maintains a certain advantage. Decision makers will weigh risk in a globally integrated manner and over a time horizon to understand how opportunities that reduce risk in one time horizon, CCMD, or Service, may lead to accepting increased risk in another. During evaluation, a decision maker may identify opportunities by accepting more “Likely, Modest” consequence events, compared to “Very Unlikely, Extreme” consequence events from the same threat, despite the fact that they fall into the same *Moderate* risk contour based on Figure 5. This is why it’s important that decision makers consider risk not just one dimensionally, but also consider time in addition to consequence and probability.

(a) Acceptable. An event where certain risks remain low enough that additional risk reduction efforts are not required.

(b) Unacceptable. The risk posed by a certain event is too high to pursue a desired activity without risk mitigation efforts.

d. Risk Management (Pillar 4). This pillar focuses on designing, implementing, and monitoring risk decisions. Risk management is an iterative process requiring periodic review to ensure decision maker's action achieves the anticipated residual risk and meets future milestones aligned to strategic priorities. Residual risk is the risk that remains after a decision maker chooses to accept, avoid, mitigate, or transfer risk. It is important to recognize that zero risk is unattainable with the existence of a threat or hazard. Risk management decisions are made as a matter of strategies, policies, operations, or tactics. Careful consideration of the various drivers of risk aid in decision making.

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

(2) Avoid. Forgo the activity that would produce unacceptable risk or remove the item of value that could be damaged due to unacceptable risk.

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

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

e. Risk Communication (Continuous Component). Risk communication is at the core of any successful effort to appraise and manage risk and is continuous during JRAM execution. Effective communication between risk stakeholders reduces misunderstandings and potential surprises. For example, identifying sources and drivers is critical for contextualizing the risk of a given event. Further communicating the drivers, as well as any assumptions involved, as early as possible when communicating risk will enable all stakeholders to understand the scope of the risk involved. It is critical to enhancing dialogue and creating confidence in the outcomes. This manual standardizes a common risk lexicon to facilitate effective communication. Senior leaders must illustrate risk levels such as *Significant* or *High* with detailed analysis.

(1) Risk Statement. Risk statements are developed for every known or expected harmful event and better inform risk management decisions. Risk statements should avoid ambiguity by assessing the harmful event bounded by known time horizons, probability, consequence, and risk level, and by specifying the type of risk or risk sub-set.

f. Risk Opportunity (Continuous Component). As appropriate, when working through each pillar of risk, assessors should consider where risk framing, assessment judgment, and management options may enable opportunities that set conditions to gain a relative advantage. This starts with the framing and assessment pillars, where assessors can examine risk with an eye towards identifying opportunities. This opportunity lens is most relevant, however, in the judgment and management pillars. In theory, if decision makers appropriately determine the degree of acceptable risk and manage it accordingly, they can simultaneously create space for opportunities that achieve milestones aligned to strategic priorities by setting the conditions. Moving through the risk analysis process with attention to opportunity encourages the Joint Force to continuously look for ways to make choices in addressing risk that reflect a global perspective of defense priorities. Risk is not inherently the presence of a threat, but can also create or expose opportunities to exploit.

An Example of Writing an Effective Risk Statement

There is a “[*Probability Level*]” probability that [*harmful event*] in [*time horizon*] from [*threat/hazard*] will result in “[*Consequence Level*]” consequence. This poses [*Risk Level*] risk to [*item/idea valued or objective*].

For example, “There is a ‘Likely’ probability that an attack in the next 8-12 months from the adversary will result in ‘Major’ consequence (between 5–10 casualties and \$20–\$30 million in property loss). This poses *Significant Military Risk* (Risk-to-Mission) to our execution of GCP-X.”

4. Other Considerations

a. Several major challenges to successful risk analysis exist:

(1) Complexity. Difficulty in establishing cause and effect relationships and intervening variables. The effect of a complex system comprised of multiple sources and drivers of risk can have a synergistic effect in which the overall risk level will be higher than the summation or average of individual risk levels.

(2) Uncertainty. Human knowledge is inherently incomplete and appraisals require assumptions. Moreover, the future strategic environment is susceptible to a degree of randomness (lending itself to the occurrence of a strategic deviation) that cannot be modeled using probabilistic analysis. Using a risk contour graph to determine a risk level is best thought of as having a small amount of variance, visualized as an ellipse rather than as a precise

point. Across a long-term time horizon, the area of uncertainty would be greater than over a near- or mid-term risk assessment.

(3) Ambiguity. Stakeholders may not agree on the exact problem or source of risk because multiple legitimate interpretations exist. Thus, the degree of confidence in any risk analysis is based on the availability of relevant data, the number of variables, and assessors' depth of knowledge. Scenario planning or war-gaming that considers multiple interpretations of the available information may prove helpful in resolving ambiguity.

(4) Volatility. The rate of change of the environment, meaning even the most current data may not provide an adequate context for decision making. Volatility tends to decrease as risk is assessed above the tactical echelon.

(5) Bias. Assessors can be susceptible to many forms of bias when conducting risk analysis. Awareness of the various cognitive biases that may influence an assessment helps refine a process that strives for objectivity. It is important to explicitly identify assumptions that feed assessments so that the analysis can be reviewed for bias. Bias may be countered by enlisting multiple stakeholders to review assumptions and assessments. Alternatively, a "red-team" charged with challenging assumptions serves as another method for countering bias.

(6) Allies and Partners. Relationships with allies and partners can both increase and decrease risk. Allies and partners may increase risk if they are unwilling, unable, or choose not to deliberately act to recognize or manage their own risk, leading to greater vulnerability to U.S. military or military strategic objectives. Conversely, allies and partners may decrease risk by revealing gaps in risk assessments and aiding in risk management.

(7) Time. The time horizon is critical and takes into account how to balance risk over time. Decisions to manage risk today will affect risk exposure in the future. Conversely, making decisions that focus on mitigating potential Future Risk may increase risk in the present or near term. Figure 6 shows a generic example of how the level of risk may decrease over three time horizons (i.e. *High Trending Down*). With the example below, the risk assessed within the 0–3 year time horizon has moved to the *Moderate* level within the 2–7 year time horizon. This aligns with the *Trending Down* modifier placed on the 0–3 year time horizon, establishing a *Moderate* risk level by the 2-year point. By the 5–15 year time horizon, this example visualizes the successful application of risk mitigation within the 0–3 year time horizon. The number and interval of time horizons should be standardized within a process by the risk owner. As this graphic visualizes, risk is not linear and should not be bounded by a linear way of thinking. Decision makers must consider the trending direction of risk

when choosing to accept, avoid, mitigate, or transfer it. It is important to keep in mind that uncertainty increases the further out in time that risk is assessed during analysis.

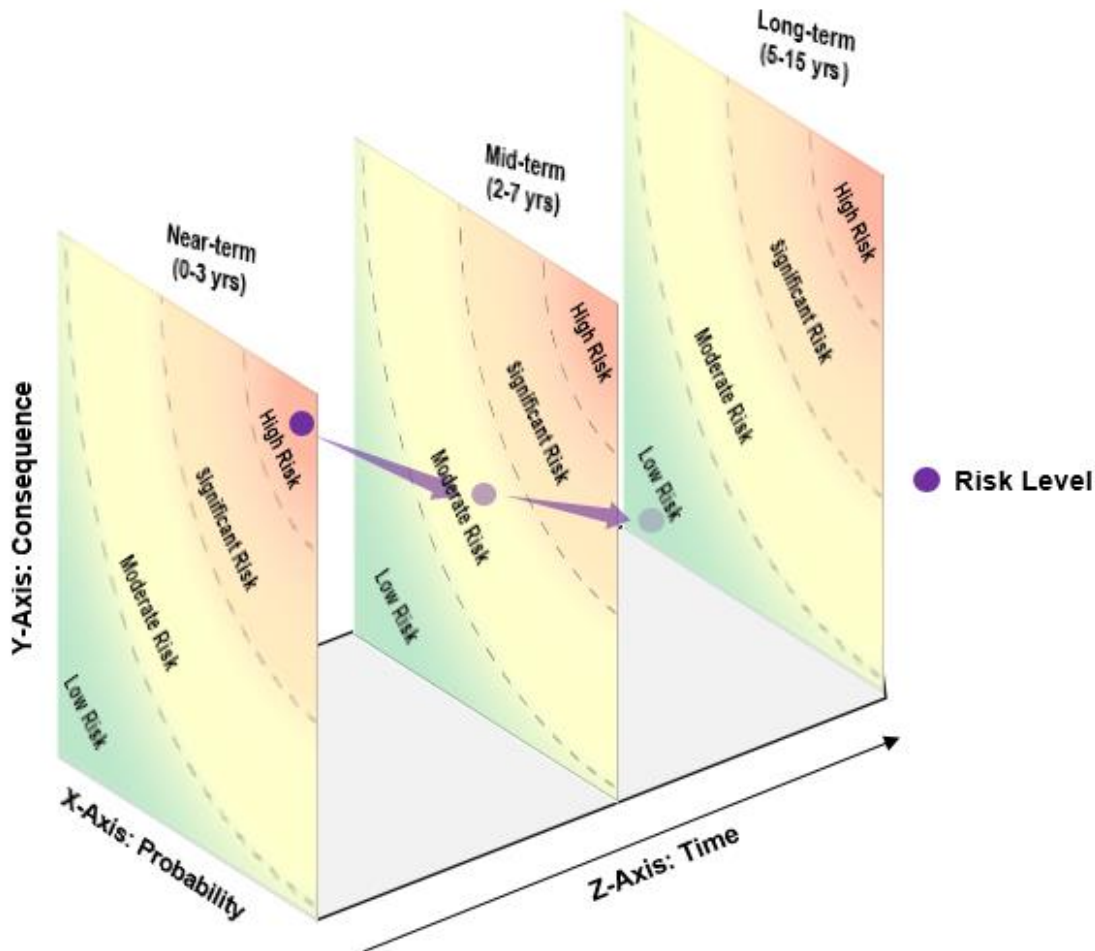


Figure 6. Risk Across Strategic Continuum Time Horizons

Figure 6 depicts how risk may change over time horizons. In the near-term, there is *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, there is *likely* probability and *modest* consequences to a harmful event occurring. In the long-term, 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 consequences of risk may become less certain over time.

(8) Global Integration. A globally integrated approach to risk is fundamental to understanding how accepting risk by one CCMD or Service may increase or decrease risk for other CCMDs or Services (Figure 7). Decision makers will be intentional about how they choose to accept, avoid, mitigate, or

transfer risk so that their choices reflect strategic priorities. While CCMDs and Services independently focus on risk to achieving their particular objectives, they must balance this with an understanding of the globally integrated risk perspective. This is due to strategic guidance possibly directing one CCMD or Service to accept increased risk because it can better address it or that risk is considered a lower priority than risks faced by another CCMD or Service. In this way, risk may be prioritized in a constrained resource environment to align with strategic priorities. A globally integrated approach to risk emphasizes the need for communication up and down the chain of command to ensure risk analyses across CCMDs and Services are not solely examined in isolation.

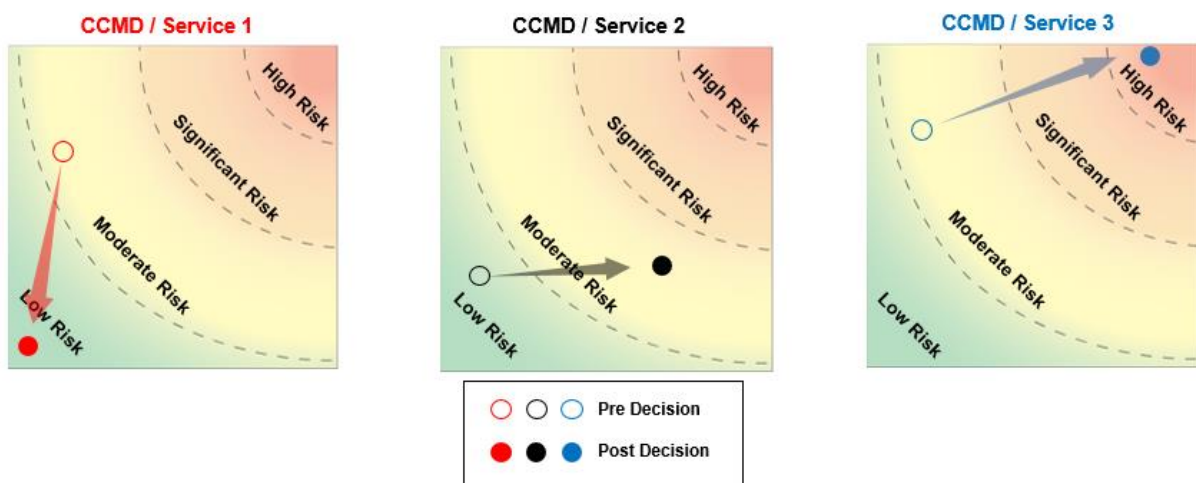


Figure 7. Globally Integrated Approach to Risk

(a) Figure 8 combines a globally integrated approach to risk with time horizons, which affords 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 for CCMD 2 and Service 1. Of greater note, risk for Service 1 will continue to increase across time horizons reaching *High* risk in the third time horizon.

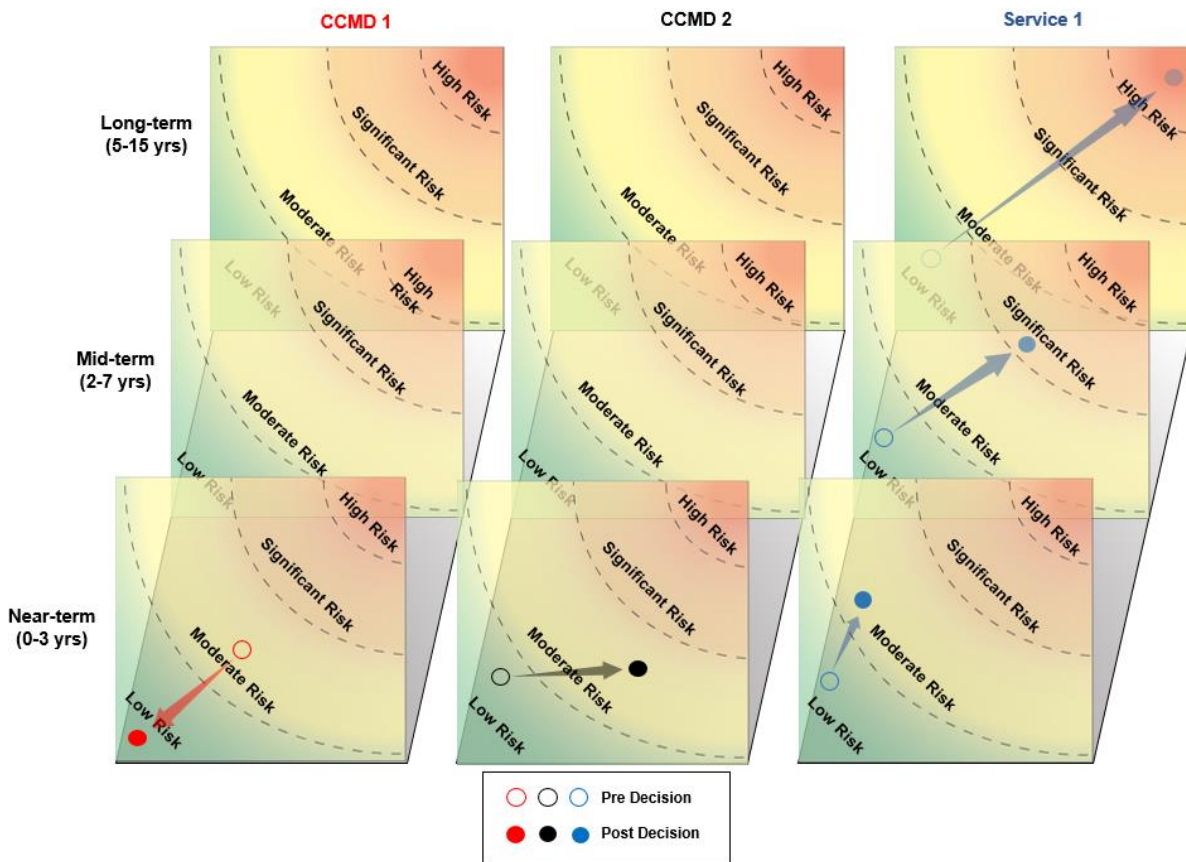


Figure 8. Globally Integrated Time Horizons

(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. Opportunity is not the absence of risk, but the space for decision makers to proactively offset the risk associated with a known harmful event to maintain an advantage.

“While risk is often portrayed mathematically, our response to risk is more often instinctive. Understanding the factors that drive how we think about and act upon risk is critical.”

General Stanley McChrystal

(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

UNCLASSIFIED

CJCSM 3105.01B
22 December 2023

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, domains, and over time.

UNCLASSIFIED

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. 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. Enclosure C examines Risk-to-Strategy and drives risk application across corresponding assessments across the JSPS. Risk-to-Strategy is the aggregate risk across the DoD enterprise that provides an assessment of the risks associated with the Joint Force’s execution of the strategy. The Global Force Management (GFM) and the CRA are examples of processes that communicate Risk-to-Strategy within the JSPS. Both the CRA and GFM processes have adopted the methodology framework from Enclosure B that is discussed herein, and can be used as examples for all Joint Force risk-related processes.

2. JRAM Application to Global Force Management. The Global Force Management Implementation Guidance (GFMIG) is the SecDef’s policy for the GFM processes. SecDef decisions on directed readiness, assignment, and allocation require a clear understanding of the globally integrated risks. The goal remains to fully inform the SecDef of the risks associated with the sourcing options to support a decision. The decisions involve balancing the risk(s) to force with the risk(s) to mission to use the Joint Force effectively and efficiently in executing the NDS, current operations and military activities, and future contingencies. CCMDs generally assess risks to mission and the Services and other force providers assess Risk-to-Force. Risk-to-Mission and Risk-to-Force are explained in more detail in the following paragraphs discussing risk in the context of the CRA. In assessing risks, CCMDs and force providers should recognize the finite nature of the Joint Force. A decision to use a force for current operations or military activities may reduce future readiness and availability thus increasing operational risk to multiple campaign and contingency plans.

- a. Adopting the risk assessment pillar from the methodology, assessors

across the Joint Force use the Military Risk Consequence Assessment Matrix in Figure 9, in addition to the JRAM probability levels, to help frame the discussion on risk. In Figure 9, each row presents a driver 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 facilitates a picture of Military Risk consequences using common metrics for the Joint Force. However, the risk analysis is not limited to the metrics shown in Figure 9. CCMDs, Services, and force providers should also consider Service red lines and any other metrics or analysis that facilitate a thorough assessment and enable communicating the risks.

b. In accordance with the GFMIG, GFM allocation sourcing recommendations, with the associated risks, are presented to the SecDef in the SecDef Orders Book (SDOB). The SDOB timelines and procedures are detailed in CJCSM 3130.06C, 7 March 2021, "GFM Allocation Policies and Procedures."

c. Readiness reporting is directly (and inversely) related to risk. As such, readiness assessments in Defense Readiness Reporting System (DRRS), Status of Resources and Training System, and Directed Readiness Tables provide the foundation for risk assessments and impact of decisions related to resourcing and authorities, as well as the trade-off between Risk-to-Mission and Risk-to-Force. Readiness assessments also provide insight into ongoing and potential mitigation efforts.

3. JRAM Application to Force Readiness Reporting. For Force Readiness Reporting, the DRRS-Strategic (DRRS-S) provides the CJCS and SecDef a comprehensive means of assessing the readiness of the Joint Force to meet its assigned missions. Commanders using risk assessment methodology and the Military Risk Matrix in Figure 9 identify the risks to mission accomplishment framed in terms of both capability and capacity shortfalls that threaten mission success. Commanders consider capability and capacity shortfalls of the forces assigned and any applied mitigations to determine the overall expected consequence level and Risk-to-Mission accomplishment in order to provide information to the CJCS and Joint Staff to make recommendations and the SecDef to make decisions regarding sourcing, force structure, and designed capabilities. The commander must use judgment and standardized metrics to assess the Joint Force. However, the risk analysis should not be limited to the ability of the commander's headquarters to accomplish the mission, but that of the forces assigned under the headquarters to meet their assigned missions. The commander should include this assessment and any other metrics or analysis within DRRS-S to facilitate leadership decision making and broader risk assessment as it pertains to executing strategic guidance.

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	Stress on AC Force (D2D)	D2D > 1:3	1:3 > D2D ≥ 1:2.5	1:2.5 > D2D ≥ 1:2	D2D < 1:2
		Stress on RC Force (M2D)	M2D > 1:5	1:5 > M2D ≥ 1:4	1:4 > M2D ≥ 1:3	M2D < 1:3
		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)
	JCIDS / 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-McCurdy)	Program failure; zeroed out (de-funded)
	JCIDS / 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 9. Military Risk Consequence Assessment Matrix

4. Chairman's Risk Assessment. The Fiscal Year 2000 National Defense Authorization Act amended title 10, U.S. Code to establish the requirement for an annual risk assessment by the CJCS. Formally, the CJCS must provide an annual risk assessment to the SecDef and to Congress about the Military Strategic Risk to national interests and Military Risk to executing the NMS. The CJCS continually considers risk when fulfilling title 10, U.S. Code 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.

a. The Joint Staff develops the CRA final report 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 Intelligence Community. In accordance with title 10, U.S. Code, if the CJCS characterizes a baseline risk as *Significant* or higher, the SecDef is required to submit to Congress a plan for mitigating those risks. This risk management portion of the framework is addressed through the SecDef's Risk Mitigation Plan (RMP). It identifies needed adjustments to authorities, policies, priorities, operations, activities, and/or investments for each baseline *Significant* or *High* Military Strategic Risk and/or Military Risk. Figure 10 shows how the JRAM is applied to the CRA. The CRA articulates the risk details in regards to executing the NMS with the Joint Force using this JRAM as the foundation of risk judgment and communication.

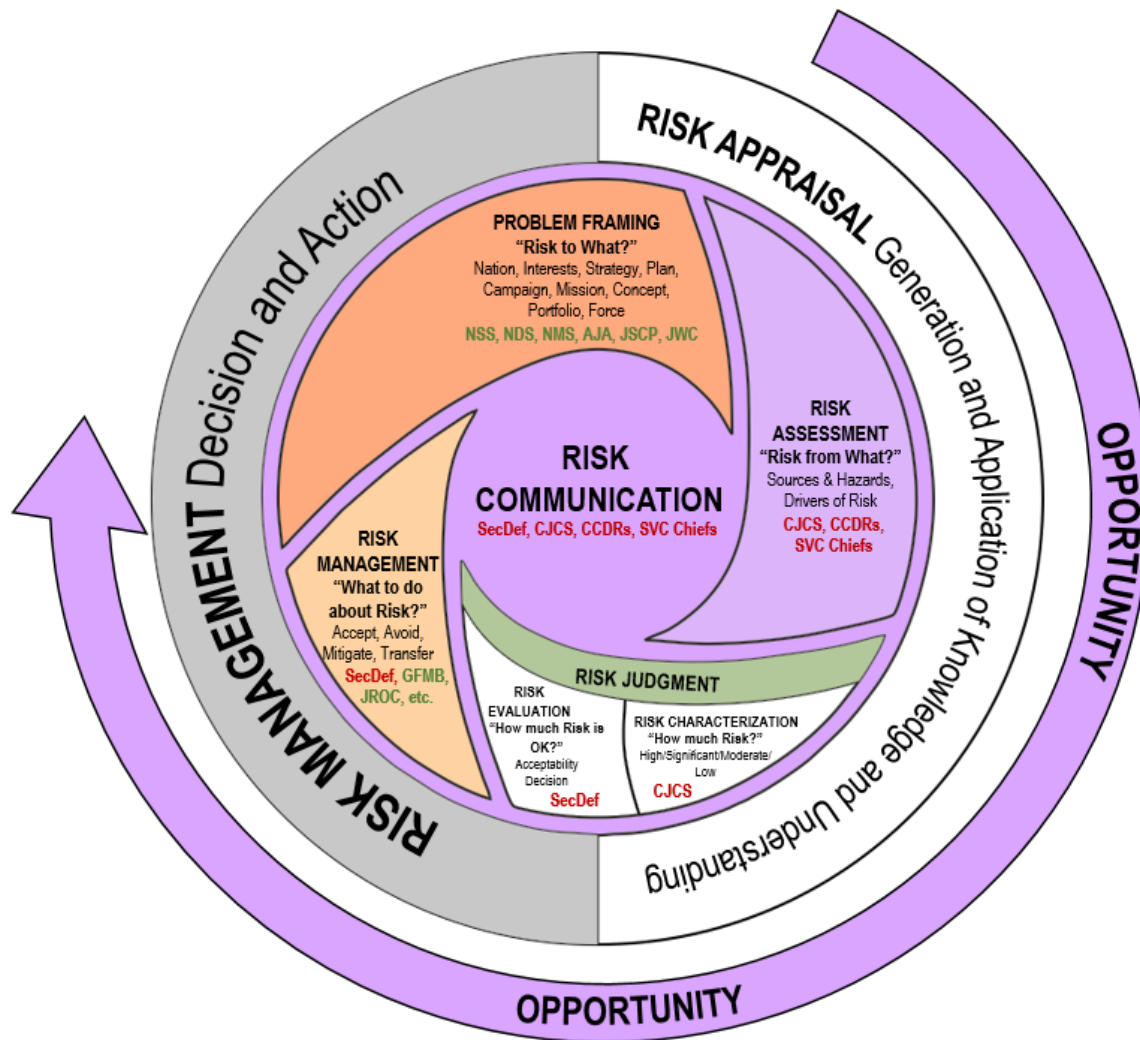


Figure 10. JRAM Framework Applied to the CRA

5. JRAM Application to the CRA

a. CRA Problem Framing. The CRA must characterize Military Strategic Risks and Military Risks as they relate to the objectives identified in the *National Security Strategy* (NSS) and NMS, respectively. Throughout the development of the CRA, the Joint Staff J-5 applies the JRAM as outlined in Enclosure B.

b. Chairman's Risk Assessment. The Joint Staff J-5, with concurrence from the CJCS, uses 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. The majority of feedback comes from JSPS processes and products including the *Annual Joint Assessment* (AJA) survey, which leverages the perspectives of each CCDR and Service Chief. The CRA considers risk across two time horizons: near-term (0–3 years) and long-term (2–15 years), which is the combination of force development and design.

(1) Military Strategic Risk. Military Strategic Risk is defined as the probability and consequence of planned and contingency events with direct military linkages causing harm to the United States and U.S. national interests. This includes harm to the U.S. population, territory, civil society, institutional processes, critical infrastructure, and interests. Military Strategic Risk has four probability levels and four consequence levels, depicted in Figure 11. As noted in the definition of Military Strategic Risk, the consequences are all tied to national interests, which are articulated in strategic guidance provided by the President, primarily through the NSS. The CJCS uses these interests as a starting point for assessment of Military Strategic Risk.

Probability of Event (P)	Consequence of Event (C) to US National Interests
Very Likely (~81-100%)	Extreme: Existential/Permanent damage
Likely (~51-80%)	Major: Catastrophic damage
Unlikely (~21-50%)	Modest: Considerable damage
Very Unlikely (~0-20%)	Minor: Confined damage

Figure 11. Military Strategic Risk Probability and Consequence Levels

(a) The strategic value of the interest being examined must be considered when determining the consequence level. It is critical that strategic values of interests do not become a function of a particular threat, but rather what could suffer the risk of a harmful event. A threat assessment should not begin before considering national interests and intensities. 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 11 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; see uncertainty.

(b) Once an assessor has determined the degree of damage (confined, considerable, catastrophic, or existential) using Figure 12, a consequence level can be obtained using Figure 13 based upon the scale or scope of the strategic value of interest. This consequence will be paired with probability over a time horizon to assess risk level during risk judgment.

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 failures of major institution or market - 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
Preservation of democratic values	- Local atrocities - Imposition of martial law by ally or partner - Democratic regression by ally or partner - Local order undermined or replaced by alternative system, neutral or antagonistic to U.S. system	- Mass atrocities - Democratic regression by key ally or partner - Local imposition of alternate value system - Regional order undermined or replaced by alternative system, neutral or antagonistic to U.S. system	- Genocide - Regional imposition of alternate value system - Emergence or powerful totalitarian nation - Elements of international order undermined or replaced by alternative system, neutral or antagonistic to U.S. system	- Global imposition of alternative value system - Rules-based international order favorable to U.S. system is replaced in total

Figure 12. Military Strategic Risk Matrix – Consequence Development

Strategic Value of Interest Scale / Scope	Harmful Event: Varying Degrees of Damage			
	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 13. Military Strategic Risk Matrix – Consequence Assessment

(2) Military Risk. There are two categories of Military Risk: Risk-to-Mission and Risk-to-Force. Risk-to-Mission is the probability and consequence of planned and contingency events causing harm to current or future military objectives. Risk-to-Force is the probability and consequence of planned and contingency events causing harm to the provision and sustainment of sufficient military resources. Both must be considered when calculating Military Risk. It involves balancing a CCMD's ability to attain steady state, current operations, and contingency plan objectives against the Services' and force provider's ability to support CCMD missions to achieve strategic objectives. The concepts of Risk-to-Mission and Risk-to-Force can be differentiated into four risk subsets based on source of risk and time horizon (Figure 14). Operational risk and future risk relate to Risk-to-Mission, while force management risk and institutional risk relate to Risk-to-Force. The time horizon will remain subjective based on strategic trends, threats, and guidance provided by the CJCS and policy when informed by Risk-to-Strategy. Generally, the Joint Force considers risk in relation to three time horizons: near-term (0–3 years), mid-term (2 – 7 years), and long-term (5–15 years).

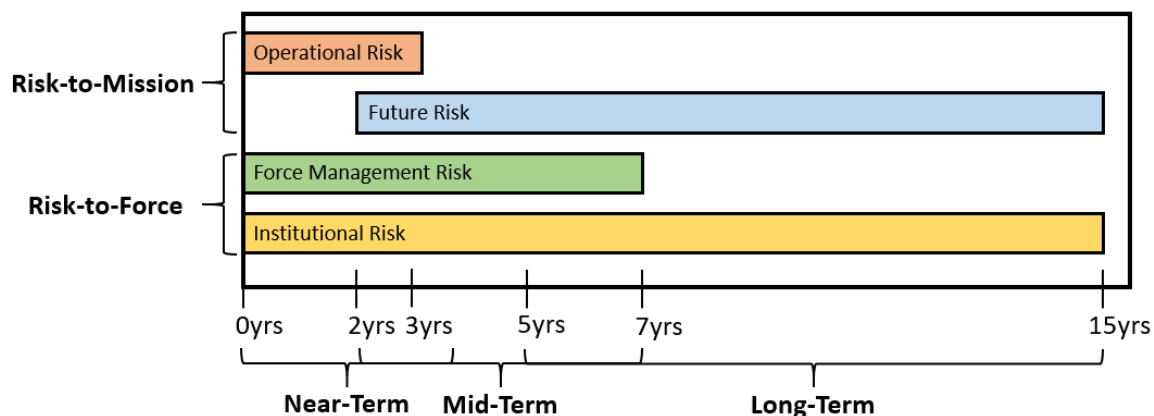


Figure 14. Military Risk Subsets over Time Horizons

(a) Risk-to-Mission

1. Operational risk is a function of the probability and consequence of failure to achieve mission objectives while protecting the force from unacceptable losses. 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, material, and financial costs. 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.

2. Future Risk during Risk-to-Mission articulation is a function of the probability and consequence of a known harmful event that causes failure to meet current and projected future strategic and 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 future risk. Leaders must consider the risk managed in the near-term versus the mid- or long-term in decision making.

(b) Risk-to-Force

1. Force management risk is a function of the probability and consequence of not maintaining the appropriate force generation balance ("breaking the force"). 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 (e.g., "fight tonight" on the Korean peninsula) to 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 discipline, and the choices that need to be made to balance operational requirements to campaign and modernization requirements to build warfighting advantage.

2. Institutional risk is a function of the probability and consequence of the DoD failing to perform established functions. It reflects the ability of organization, command, management, and force development processes and infrastructure to plan for, enable, and improve national defense. The time horizon associated with this risk subset is much broader. All three

time categories—near-, mid-, and long-term—will impact institutional risk. It considers organization and process effectiveness, including the acquisition process and budgetary impacts, as well as program health, health of the force, and the defense industrial base.

3. Military Risk is assessed using the four probability levels and four consequence levels depicted in Figure 15. As with Military Strategic Risk, judgment is required to integrate different levels of probability and consequence during Risk Characterization.

Probability of Event (P)	Consequence of Event (C) to NMS
Very Likely (~81-100%)	Extreme - RM, Mission Failure, Objectives Unachievable - RF, No Sourcing Solutions Exist for Critical Requirements
Likely (~51-80%)	Major - RM, Objectives Minimally Achieved (consider time, priority) - RF, Shortfalls Exist for Critical Requirements
Unlikely (~21-50%)	Modest - RM, Objectives Mostly Achieved (consider time, priority) - RF, Worldwide Sourcing Solution Exist for Most Requirements
Very Unlikely (~0-20%)	Minor - RM, Mission Success, Objectives Achievable - RF, Joint Force Fully Sustained and Requirements Sourced

Figure 15. Military Risk Probability and Consequence Levels

c. CRA Risk Judgment

(1) CRA Risk Characterization. After evaluating the probability and consequence of Military Strategic and Military sources and drivers of risk, events are assigned a risk level of *Low*, *Moderate*, *Significant*, or *High* (Figure 16). Risk is additionally modified with *Trending Up* or *Trending Down* descriptors based on an assessed direction of risk over a specified

time horizon. Ultimately, the CJCS makes the final decision on risk levels conveyed in the CRA due to their role as Global Integrator.

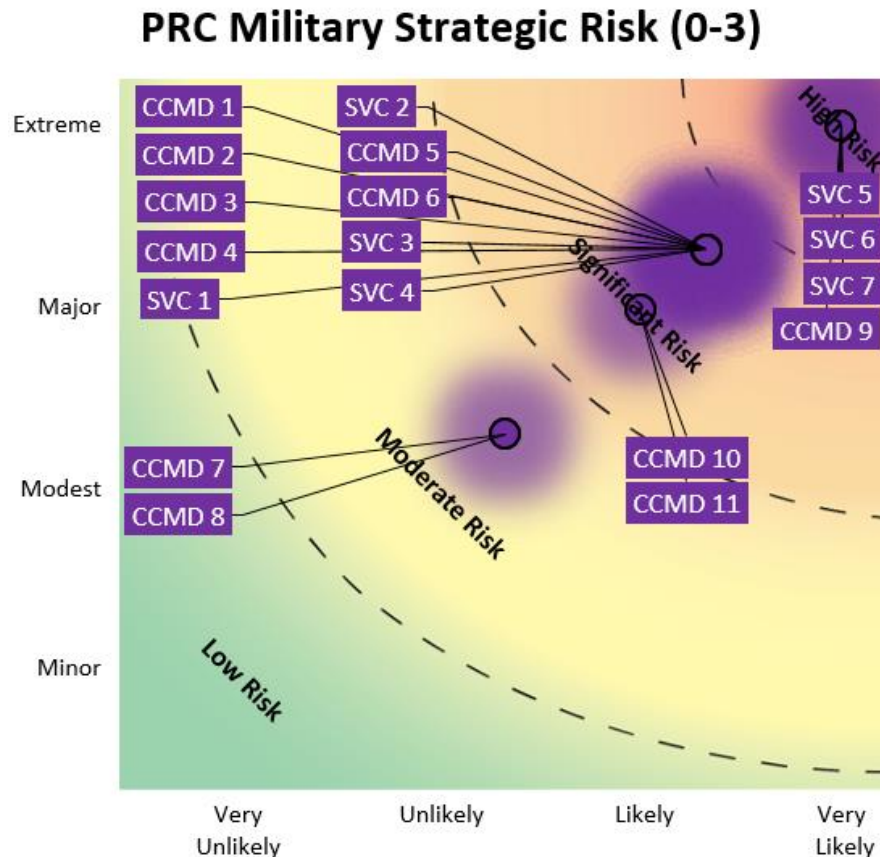


Figure 16. Example CCMD/Service Military Strategic Risk CRA Contour Plot

(a) Once all of the Military Strategic Risks and Military Risks have been characterized and approved by the CJCS, the Joint Staff J-5 finalizes the CRA and forwards it to the CJCS for signature. It is then passed to the SecDef to evaluate and manage the risk. A visual representation of a final, integrated risk contour plot is exemplified in Figure 16.

(b) The signed 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 a NMS revision should the assessment find that the strategic environment has changed and the level of risk becomes unacceptable

Chairman's Risk Assessment: Global Integration of Risk

The assessed Military Strategic and Military Risks 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 SecDef delivers to Congress with an accompanying mitigation plan.

(2) CRA Risk Evaluation

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

(b) Another major consideration during risk evaluation is to trade space between Military Strategic Risk and Military Risk. Decision makers must contemplate second- and third-order effects of risk decisions. Decisions made to manage Military Risk have the potential to increase Military Strategic Risk.

d. CRA Risk Management. The RMP is the formal means for the SecDef to explain how the DoD 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 DoD mitigates risk in many ways. Military Strategic Risk is mitigated by adjusting authorities, policies, budget, and priorities. The previously defined Military Risk subsets, Risk-to-Mission and Risk-to-Force (based on source and time horizon), help determine the most effective ways to address that type of risk.

e. 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.

6. Summary. Strategic assessments serve as the keystone for risk calculation to the Nation's strategy and 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.

UNCLASSIFIED

CJCSM 3105.01B
22 December 2023

(INTENTIONALLY BLANK)

UNCLASSIFIED

ENCLOSURE D

RISK REFERENCE 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) 3100.01 Series, “Joint Strategic Planning System,” 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 3141.01 Series, “Management and Review of Campaign and Contingency Plans.”

f. CJCSI 3401.01 Series, “Joint Combat Capability Assessment.”

g. CJCSI 3401.02 Series, “Force Readiness Reporting.”

h. CJCS Manual 3130.06 Series, “Global Force Management Allocation Policies and Procedures,” 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: Enterprise Risk Management, DAO 216-20.

b. National Institute of Standards and Technology (NIST): *Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems*. NIST Special Publication 800-37, Rev 1.

c. Office of Management and Budget (OMB): OMB Circular A-123, *Internal Control Systems*, establishes enterprise risk management approaches.

d. Department of Homeland Security (DHS): *DHS Risk Lexicon*, September 2010. The DHS Risk Lexicon is part of that Department’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.

5. Risk in the Department of Defense

a. Office of the Chief of Naval Operations Instruction 3500.39 Series, “Operational Risk Management.”

b. Marine Corps Order 5100.29 Series, “The Marine Corps Safety Management System.”

c. Department of the Army Pamphlet 385-30, “Risk Management.”

d. Air Force Instruction 90-802, “Risk Management.”

e. DoD Instruction 6055.01, 14 October 2014, “DoD Safety and Occupational Health (SOH) Program.” This document provides overarching DoD 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 DoD 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. DoD Instruction 8510.01, “Risk Management Framework for DoD Information Technology,” describes policy and procedures applicable to the integrated enterprise-wide structure for cybersecurity risk management.

h. The GFMIG, section IV amplifies how the risk framework in this manual is to be applied to the GFM allocation process.

i. “Risk of Strategic Deterrence Failure” (RoSDF) is the assessment U.S. Strategic Command conducts for the DoD to meet its *Unified Command Plan*-assigned Strategic Deterrence mission. RoSDF assesses the risk of an attack or series of attacks, regardless of means, which causes or was intended to cause catastrophic or existential effects on U.S. vital interests that could drive consideration of a strategic response.

UNCLASSIFIED

CJCSM 3105.01B
22 December 2023

(INTENTIONALLY BLANK)

UNCLASSIFIED

GLOSSARY

PART I-ABBREVIATIONS AND ACRONYMS

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

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
CRA	Chairman's Risk Assessment
DHS	Department of Homeland Security
DoD	Department of Defense
DRRS	Defense Readiness Reporting System
DRRS-S	Defense Readiness Reporting System-Strategic
DRT	Defense Readiness Tables
GCP	Global Campaign Plan
GFM	Global Force Management
GFMIG	Global Force Management Implementation Guidance
IRGC	International Risk Governance Council
ISO	International Organization for Standardization
JP	Joint Publication
JRAM*	Joint Risk Analysis Methodology
JSPS*	Joint Strategic Planning System
NIST	National Institute of Standards and Technology
NMS	National Military Strategy
OMB	Office of Management and Budget
RF	Risk-to-Force
RM	Risk-to-Mission
RMF	Risk Management Framework
RMP	Risk Mitigation Plan
RoSDF	Risk of Strategic Deterrence Failure

UNCLASSIFIED

CJCSM 3105.01B
22 December 2023

SecDef
SORTS

Secretary of Defense
Status of Resources and Training System

TPFDD

Time-Phased Force Deployment Data

PART II-DEFINITIONS

Unless otherwise sourced, terms are for this document only.

Drivers of Risk – Factors that act either to increase or decrease the probability or consequence of risks arising from various sources.

Hazard – Security, environmental, demographic, political, technical, or social conditions with potential to cause harm.

Harmful Event – A foreseeable event in the future, singular or persistent, that harms the item or idea that is valued. It requires, at minimum, a source and driver of risk. For unforeseen events, or strategic deviations, refer to uncertainty.

Joint Risk Analysis Methodology (JRAM) – A risk framework providing a consistent, standardized way to appraise, manage, and communicate risk.

Joint Strategic Planning System (JSPS) – The primary means by which the CJCS 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 SecDef and the President.

Military Risk – The estimated probability and consequence of the Joint Force's projected inability to achieve current or future military objectives (Risk-to-Mission), while sustaining sufficient military resources (Risk-to-Force). *High* Military Risk describes a very likely probability of mission failure, or a lack of sourcing solutions for critical requirements. *Significant* Military Risk describes a likely probability of only achieving partial objectives, or that shortfalls exist for critical requirements. *Moderate* Military Risk describes a likely probability of achieving most but not all objectives, or that worldwide sourcing solutions exist for most requirements.

Military Strategic Risk – The estimated probability and consequence of current and contingency events with direct military linkages to the United States. This includes the U.S. population, territory, civil society, institutional processes, critical infrastructure, and interests. The consequences align to the national interests articulated in strategic guidance provided by the President, primarily through the *National Security Strategy* (NSS). *High* Military Strategic Risk describes an event that would very likely cause existential damage to national interests; *Significant* risk describes a likely catastrophic hazard to national interests; and *Moderate* risk describes an unlikely considerable hazard to national interests.

Problem Framing – First pillar in the JRAM, generating a common understanding of the risk issue(s), major assumptions, and procedural rules.

Risk – Risk is the probability and consequence of an event causing harm to something valued, classified within one of four risk levels (*Low, Moderate, Significant, or High*).

Risk Acceptance – An informed decision to act without conducting risk mitigation efforts.

Risk Appraisal – A component of the JRAM, during which knowledge and understanding is generated.

Risk Assessment – Second pillar in the JRAM, during which sources of harm are linked with likely consequences and expected probability.

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 Judgment, during which events are assigned a level of risk.

Risk Communication – A component of the JRAM encompassing the exchange of risk perspectives across processes and among leadership.

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

Risk Judgment – Third pillar in the JRAM, composed of Risk Characterization and Risk Evaluation, aimed at determining acceptability of a risk.

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

Risk Management – The fourth pillar of the JRAM where risk decisions to accept, avoid, mitigate, or transfer risk are designed, implemented, and monitored.

Risk Mitigation – An action that reduces the risk consequence or probability.

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

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 valued item or idea.

Threat – A state or non-state entity with capability and intent to cause harm.

UNCLASSIFIED

CJCSM 3105.01B
22 December 2023

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED



UNCLASSIFIED