CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-5 CJCSM 3105.01A
DISTRIBUTION: A, B, C 12 October 2021

JOINT RISK ANALYSIS METHODOLOGY

References:
See Enclosure D

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 (JF) 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 JF processes, illustrates how risk connects these efforts, and provides a framework for the JF 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 which supports the JSPS.

2. Superseded/Cancellation. CJCSM 3105.01, "Joint Risk Analysis," 14 October 2016 is hereby superseded.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 can apply the principles outlined in this manual across their spectrum of responsibilities.

4. Procedures. See Enclosures A through C.

5. Summary of Changes. The previous Enclosure D was removed as it is included in the latest revision of JSPS, with necessary information moved to Enclosure A. "Strategic Risk" has been replaced with "Military Strategic Risk"

as referenced in title 10, U.S. Code. The four steps language was changed to the four pillars, as JRAM is meant to be a framework and not a prescriptive iterative process. All figures have been updated. The Integrated Risk Matrix, Vignettes, and un-used glossary terms were removed. The rest of the changes are administrative in nature.

6. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on NIPRNET. 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>. JS activities may also obtain access via the SIPR Directives Electronic Library Websites.

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

For the Chairman of the Joint Chiefs of Staff:

ANDREW P. POPPAS, LTG, USA
Director, Joint Staff

Enclosures
- A – Risk and the Joint Force
- B – Joint Risk Analysis Methodology
- C – Chairman's Risk Assessment
- D – References and Other Risk Documents
- GL – Glossary

CJCSM 3105.01A
12 October 2021

TABLE OF CONTENTS

LIST OF FIGURES

ENCLOSURE A

RISK AND THE JOINT FORCE

1. Introduction. The JRAM presents a common methodology, consistent with risk best practices, for the JF to conduct risk appraisal and risk management comprehensively throughout the JSPS. JRAM is also a useful reference to facilitate consistency across the DoD to enhance risk communication and decision making. 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 (includes characterization and evaluation), and risk management. By applying this methodology, the JF can use the same terms and processes to communicate military strategic risk (risk to national interests) and military risk (risk to executing the NMS). The methodology described in this manual, coupled with military judgment, helps determine risk levels and mitigation strategies to facilitate risk informed decisions.

2. JSPS and Risk. Commanders and staffs consider threats daily that affect operations in relation to current and future threats and their own forces. The cyclical nature of the JSPS requires the Joint Staff, CCMDs, and Services to use the JRAM when appraising the risk associated with these threats. Calculating risk throughout the JSPS will facilitate the best decisions and recommendations as the JF executes its title 10, U.S. Code requirements, functions, and products.

a. Leaders and staffs must identify and define “risk to what, to whom” in military terms. They will articulate “risk to what, to whom” after considering risk inputs from many organizations. Figure 1 displays the nested direction and missions and their sources (left) along with the nested 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.

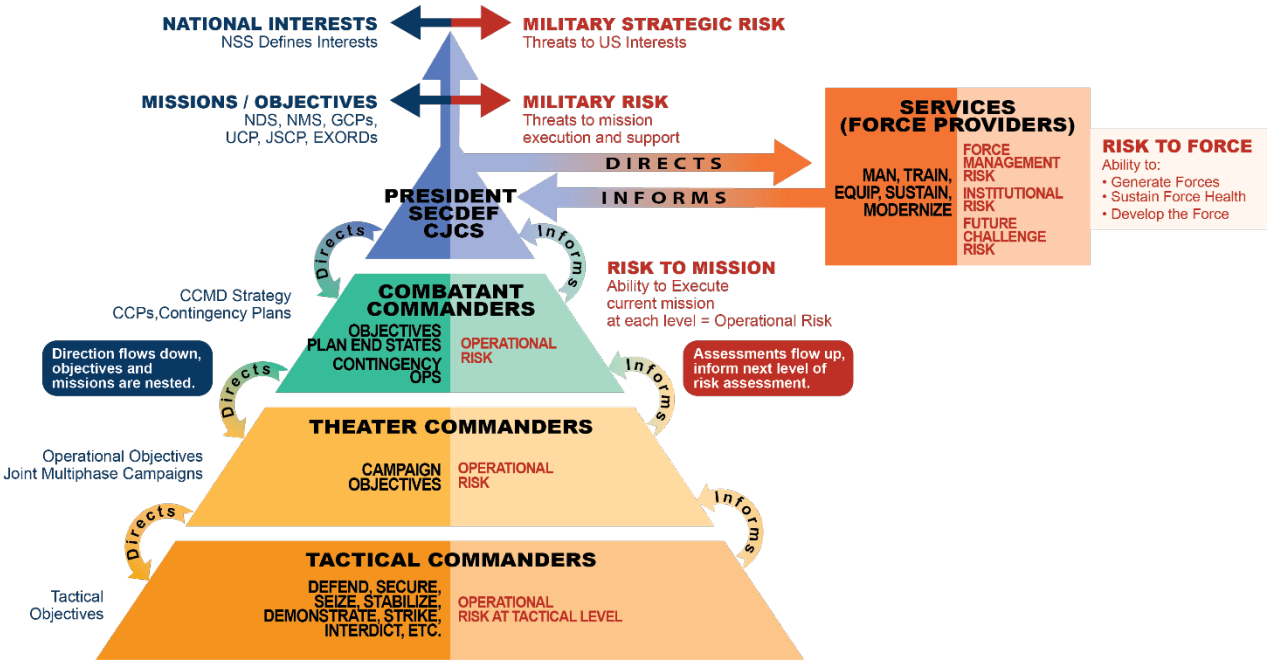

Figure 1. Organizations and Risk

3. Summary. The JF must consider risk globally to allocate resources, set priorities, and achieve national military objectives. This is done primarily through the JSPS processes and products and through Global Force Management (GFM). As each process tackles problem sets, commanders and staffs will use risk analysis to provide the best military advice possible in pursuit of executing an effective strategy. Appraising, managing, and communicating global risk lays the foundation and priorities to employ, manage, compare, and develop the JF to meet and prioritize national military objectives.

ENCLOSURE B

JOINT RISK ANALYSIS METHODOLOGY

1. Introduction. Risk is the probability and consequence of an event causing harm to something valued. Risk is classified within one of four risk levels (low, moderate, significant, or high). Accurately appraising, managing, and communicating risk at the appropriate level of responsibility allows leaders and staffs to make informed decisions across disparate processes. The JRAM provides a consistent, standardized framework to appraise, manage, and communicate risk. Risk appraisal is fundamentally a qualitative process incorporating a commander's judgment, but can quantitatively express probability and consequence when appropriate. Risk is specific to the time in which an event occurs, and the probability and consequence should be described within a time horizon. This framework is flexible enough that risk related processes can adapt portions of it, but the foundational elements—probability, consequence, time, global integration, and risk level—remain constant. This is to minimize bias and enhance comparisons across the JF.

2. Framework. The JRAM framework consists of three major components and four pillars to address risk comprehensively (Figure 2).

a. Components

(1) Risk Appraisal. Generation of knowledge and understanding.

(2) Risk Management. Decisions and actions to accept, avoid, mitigate, or transfer risk.

(3) Risk Communication. The exchange of risk perspectives across processes and among leadership.

b. Pillars

(1) Problem Framing. Identifying the item or idea which 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 about the risk?").

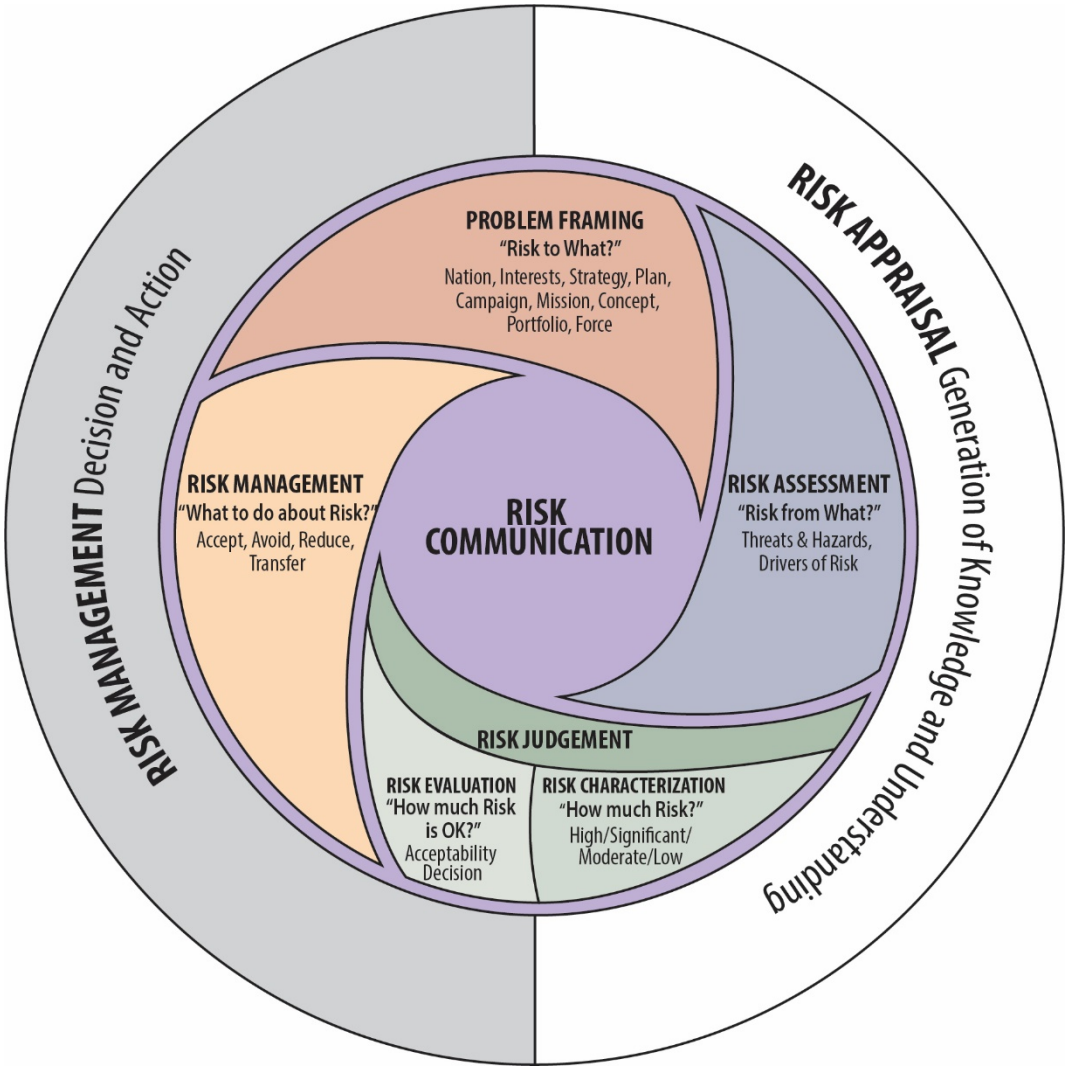

Figure 2. The Joint Risk Framework

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 which 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 process owner to define the standards (criteria, scale, terms, etc.) they will use 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 NMS continuum of strategic direction: force employment (0–3 years), force development (2–7 years), and force design (5–15 years). Strategic thoughts that do not consider time horizons undercut efforts to adapt and innovate the JF for the necessary advantages against adversaries, and make risk comparisons across commands, functions, and domains difficult. Problem framing must also express strategic thinking from a globally integrated perspective, considering CCMDs, Services, allies, partners, and non-military entities. Strategic thoughts focused on only one of these leaves risk along the seams unexamined and fails to adopt an enterprise approach to the JF increasing or decreasing risk in other areas.

b. Risk Assessment (Pillar 2). The risk assessment 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 (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. First, one must identify the sources of risk that will cause the harmful event and drivers of risk that may increase or decrease the probability or consequence.

(1) Harmful Event

(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. Actions, decisions, or security, environmental, demographic, political, technical, or social conditions with potential to cause harm.

(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 force employment (0–3 years), force development (2–7 years), and force design (5–15 years). Drivers of risk can both increase or decrease risk. A driver that may increase risk in the force employment time horizon may become obsolete or reduce risk when considered in the force development and force design time horizons. Other risk driver considerations include, but are not limited to:

1. Frequency. The number of times a threat or hazard presents in the situational environment over a given period of time.

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

3. Resilience. How quickly the JF can recover. 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. How important the thing of value is.

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 JF.

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

8. Resources. People, equipment, 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 JF, which may increase or decrease as situations escalate or de-escalate. The situational environment is always changing in response to JF, adversary, and environmental factors.

(2) Probability and Consequence. While unknown sources of risk may exist, once the assessor has identified the known sources and drivers they must determine the expected probability and consequence of occurrence 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 process owner.

(a) Probability. Probability is the determination of the likelihood of a harmful event occurring. To enable unambiguous risk communication, probability should be clearly defined in the most quantifiable manner possible. For this generic example, a four-level table helps the assessor designate level of probability of an event occurring (Figure 3). The levels "Very Unlikely" and "Very Likely" 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 Unlikely and Likely 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 operate 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.

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

Figure 3. Probability Levels

(b) Consequence. Consequence is the impact or resulting harm if the harmful event occurs. 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 "Minor" to "Extreme" should be tailored to describe specific risk scenarios. Harm is generally estimated considering vulnerability, resilience, criticality, impact, and resources.

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

Figure 4. Consequence Levels

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 supported by as many facts as possible 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. The risk level is a function of the previously assessed

Probability (P) and Consequence (C). Plotting the source of risk's assessed probability and consequence on a risk contour graph can help determine the risk level. This part of the process is subjective, and a visual depiction of the assessed probability and consequence will allow subject matter experts or decision makers to determine an appropriate risk level. The combination of probability and consequence determines the initial risk characterization. The probability and consequence levels in the following generic curve (Figure 5) are adaptable to organization's needs; however, the risk levels of low, moderate, significant, and high remain constant. Risk can be qualified by "Trending Up" or "Trending Down" based on a perceived direction of risk over a period of time.

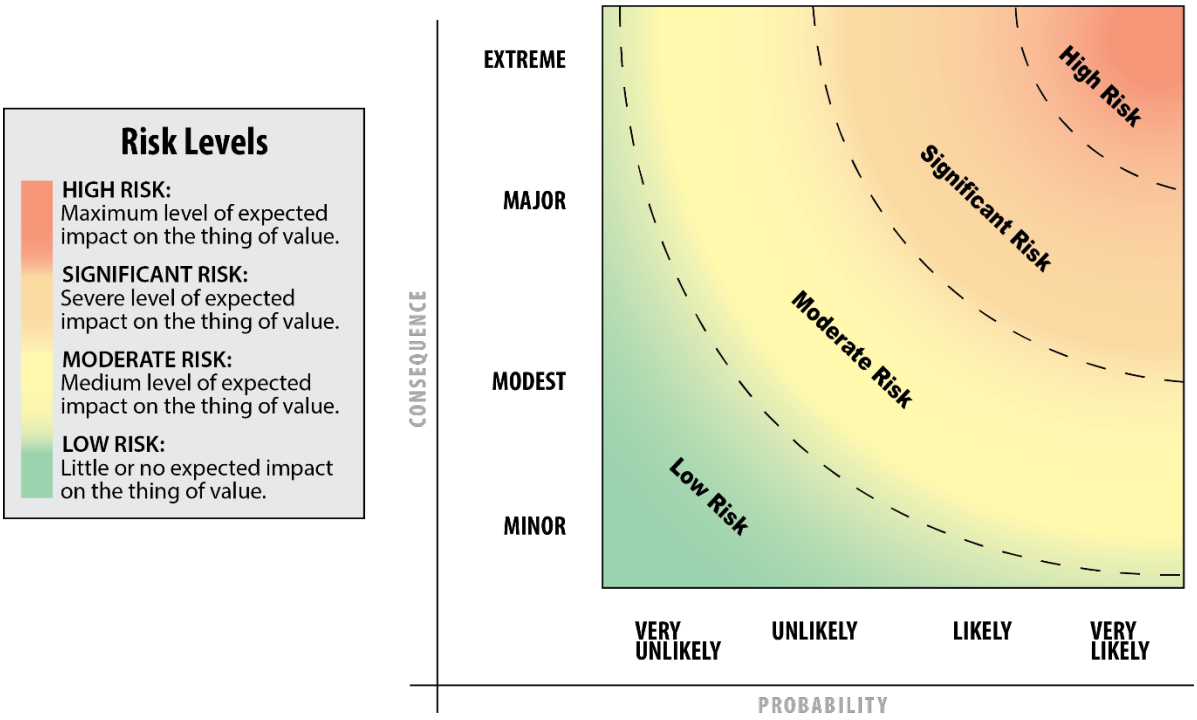

Figure 5. Generic Risk Contour

(a) Risk Statement. Some processes may benefit from a risk statement, developed for every stated harmful event to better inform the risk management component. Risk statements may avoid ambiguity by stating the harmful event, probability, consequence, and risk level bounded by any applicable time horizons. For example, "There is a significant risk to our execution of GCP-X due to a likely probability (60–70%) that the adversary will attack in the next 8–12 months. If this occurs, there will be a major consequence (between 5–10 casualties and $20–$30 million in property loss)."

(2) Risk Evaluation. During risk evaluation, a decision maker judges the acceptability of a risk, which will inform decisions on how to manage the

risk. During evaluation they may adjust probability or consequence; e.g., address more probable modest impact threats over less likely extreme threats. They also weigh risk over time, and may choose to accept risk in one time horizon to reduce risk in another. Finally, decision makers weigh risk in a globally integrated manner to understand how mitigating risk for one CCMD or Service may increase risk in another.

(a) Acceptable. An activity where certain risks remain low enough that additional risk reduction efforts are not required. Zero risk is not attainable; there will always be residual risk that remains following mitigation measures.

(b) Unacceptable. Risk is too high to pursue a desired activity without additional risk mitigation efforts.

d. Risk Management (Pillar 4). This pillar focuses on designing, implementing, and monitoring risk decisions. Decision makers may choose to accept, avoid, mitigate, or transfer risk. Acceptance and avoidance are risk decisions made as a matter of strategy, policy, operations, or tactics. Mitigating and transferring risk are components of risk mitigation.

(1) Accept. Make an informed decision to act without mitigating the risk.

(2) Avoid. Forgo the activity that would produce unacceptable risk.

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

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

e. Risk Communication (continuous during all pillars). 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. It is critical to enhancing dialogue and creating confidence in the outcomes. Senior leaders must illustrate risk levels such as “significant” or “high” with detailed analysis.

4. Other Significant Considerations

a. Five 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.

(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. Risk assessments on a Risk Contour graph are best thought of as having a small amount of variance rather than as a precise point.

(4) Volatility. The rate of change of the environment, meaning even the most current data may not provide an adequate context for decision making.

(5) Biases. Assessors can be susceptible to many forms of bias when conducting risk analysis, including the tendency to selectively seek out and analyze only information that supports conclusions they already believe (confirmation bias).

b. 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 cause increased 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. The number and interval of time horizons should be standardized within a process by the process owner. Decision makers must consider the perceived trending direction of risk when choosing to accept, avoid, mitigate, or transfer it.

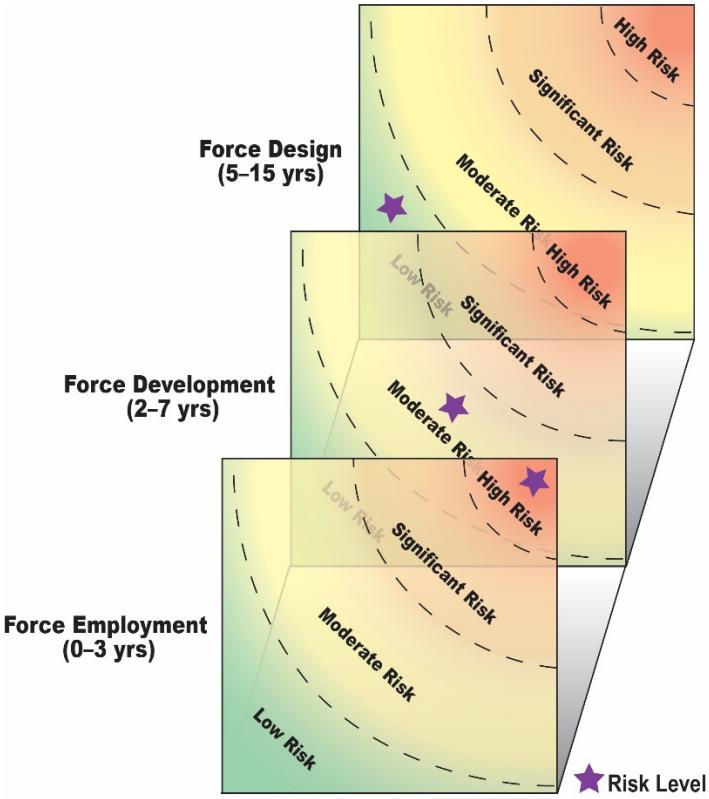

Figure 6. Strategic Continuum Time Horizons

c. A globally integrated approach to risk is fundamental to understanding how taking 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. Understanding risk as globally integrated requires an enterprise mindset. One CCMD or Service may be required 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.

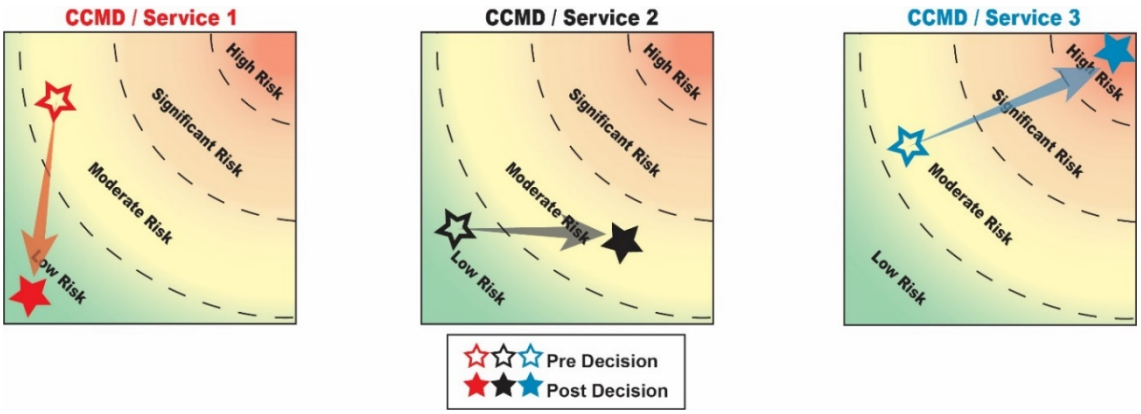

Figure 7. Globally Integrated Approach to Risk

d. Figure 8 combines time horizons with a globally integrated approach to risk, which affords an assessor or senior leader the opportunity to visually understand how risk decisions affect the JF 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. It is important to understand that in this example, risk for Service 1 will continue to increase across time horizons reaching high risk in time horizon three.

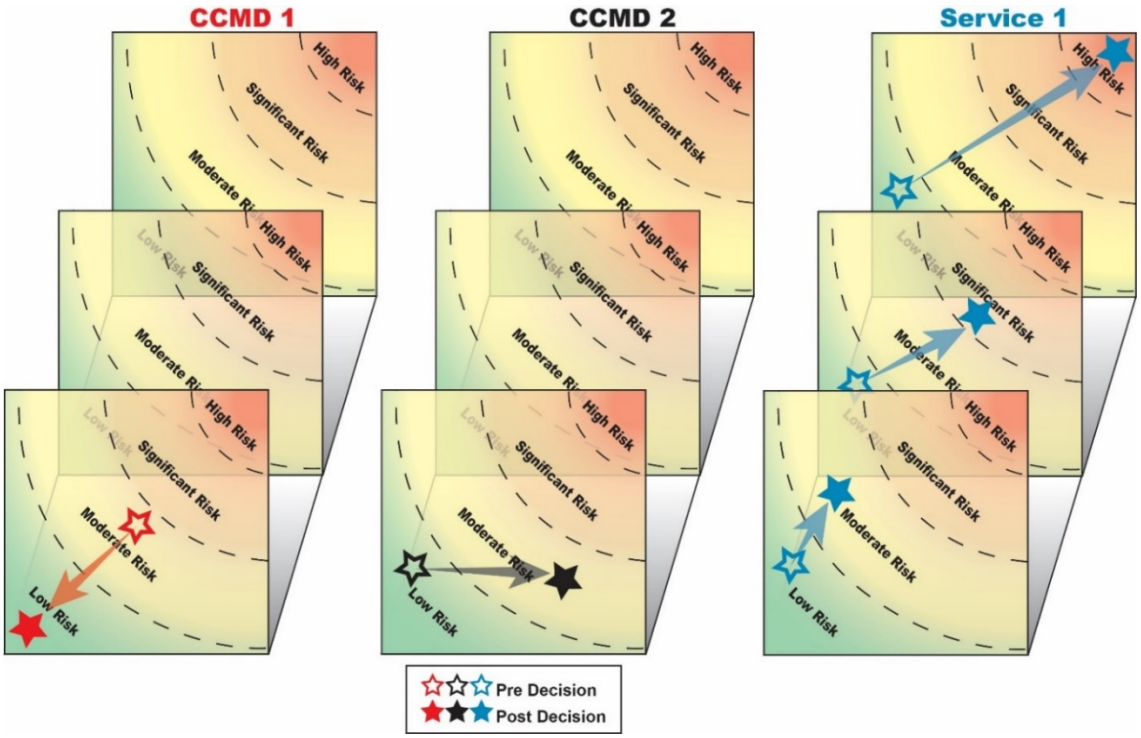

Figure 8. Globally Integrated Time Horizons

e. The challenges 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 possible) improves the overall understanding and communication of risk, ensuring that risk is comparable across regions, functions, domains, and over time.

5. Summary. Accurately appraising, managing, and communicating risk is important for decision makers across the JF, which uses the JRAM to provide a framework and establish a common lexicon to achieve these goals.

(INTENTIONALLY BLANK)

ENCLOSURE C

CHAIRMAN'S RISK ASSESSMENT

1. Introduction. Enclosure B introduced the JRAM framework and described how an organization can adapt the pillars to fit their needs, using constant risk levels (low, moderate, significant, high) to ensure standardization across risk judgements. Enclosure C adapts the JRAM framework for the CRA, and can be used as an example for all JF risk related processes.

a. The Fiscal Year 2000 National Defense Authorization Act amended title 10, U.S. Code to establish the requirement for an annual Risk Assessment of the CJCS. General Hugh Shelton published the first CRA on 6 March 2000. Formally, the CJCS must provide an annual risk assessment to the Secretary of Defense (SecDef) and to Congress about the military strategic risks to national interests and military risks to executing the NMS. The CJCS continually considers risk when fulfilling title 10, U.S. Code functions within the JSPS. Specifically, the CRA provides a risk baseline that informs assessment and advisory actions throughout the year. The CRA cuts across processes and acts as a key feedback mechanism throughout the JSPS.

b. 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 J-5 with input from the CCMDs, Services, other Joint Staff elements, the Intelligence Community, and academia. In accordance with title 10, U.S. Code, if the CJCS characterizes risks 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 Secretary's Risk Mitigation Plan (RMP). It identifies needed adjustments to authorities, policies, priorities, operations, activities, and/or investments for each significant military strategic risk or military risk. Figure 9 shows how the JRAM is applied to the CRA. The CRA articulates the risk details in regards to the Nation's strategy and JF using this methodology as the foundation.

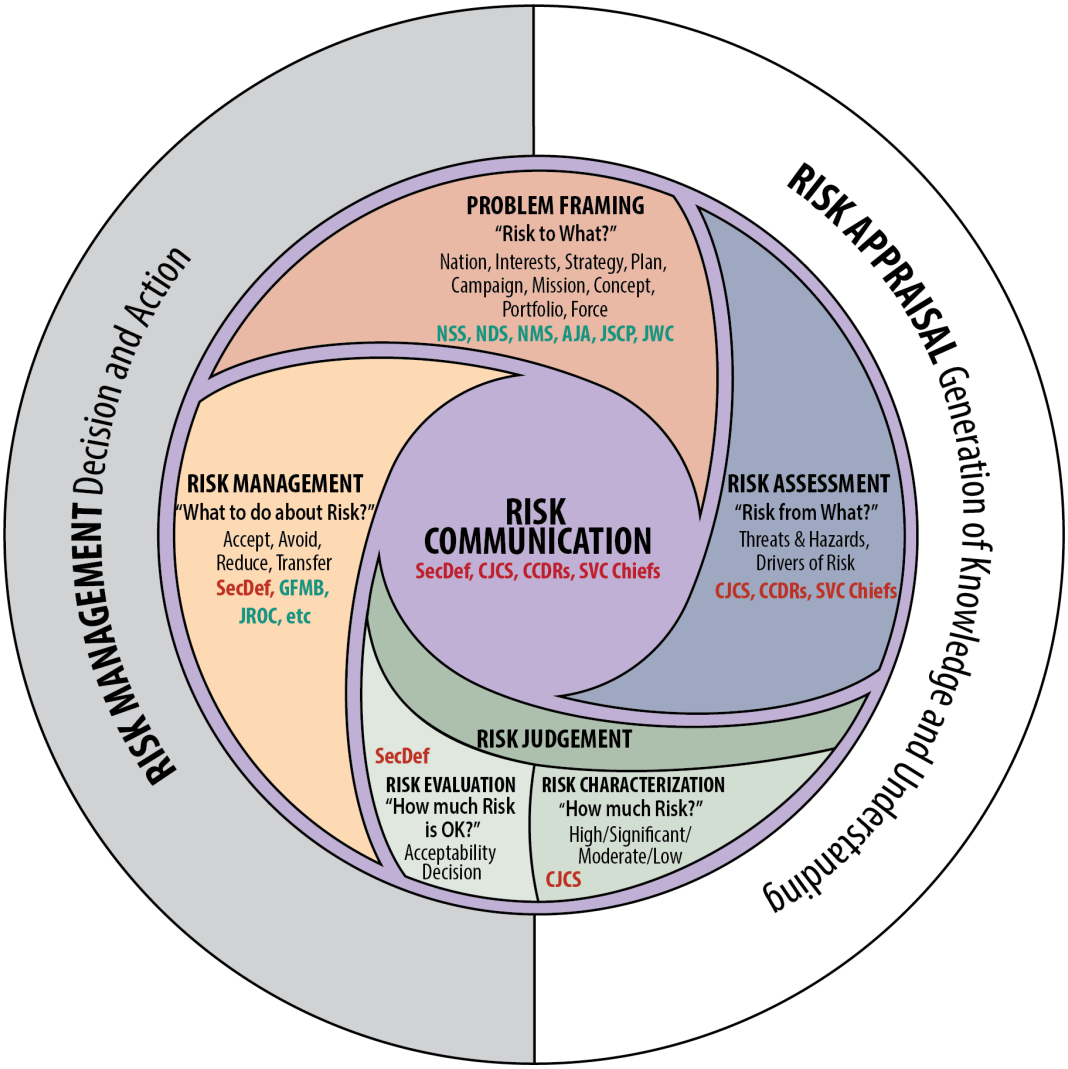

Figure 9. JRAM Applied to the CRA

2. JRAM Application

a. CRA Problem Framing. The CRA must evaluate two types of risk—military strategic risk and military risk. Throughout the development of the CRA, the Joint Staff J-5 applies the JRAM as outlined in Enclosure B.

b. CRA Risk Assessment. As part of risk assessment, the Joint Staff J-5, with concurrence from the CJCS, establishes standardized definitions, probability, and consequence levels for each type of risk. 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. The CRA considers risk from the NMS continuum of strategic direction, force employment (0–3 years), force development (2–7 years), and force design (5–15 years).

(1) Military Strategic Risk. The probability and consequence of current and contingency events with direct military linkages to the United States. This includes 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 10. 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 *National Security Strategy*. 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 10. Military Strategic Risk Probability and Consequence Levels

(a) The strategic value of the interest being targeted should be considered when determining the consequence level. It is critical that interests do not become a function of a particular threat. A threat assessment should not begin before considering interests and intensities. Doing so risks reacting to a threat with major commitments and resources devoid of any rational linkage to the relative critical value of 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 categorized as minor, modest, major, or extreme. To assist with this determination, Figure 11 frames the interest threatened and the degree of harm to that interest.

		Sources of Risk Based on damage to interest, time, resiliency			
Driver of Risk	**Strategic Value of Interest**	**Confined** Damage to interests, and/or short-term impacts	**Considerable** Damage to interests and/or mid-term impacts	**Catastrophic** Damage to interests and/or long-term impacts	**Existential** Damage to interests, and/or permanent of defining system
The Security of the U.S., its population, civil society, Allies and Partners	HLD/Vital Ally/Global Partner/Regional Other/Local	• Small Scale Contingency Ops (NEO, HA/DR) • Tactical Terror Attack (Lone Wolf) • Minor domestic civil disturbance • American hostage(s) • Loss of access • Coop 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 (9/11) • Strategic Attack on Global Domain or critical infrastructure • Concurrent widespread major domestic civil disturbances • Integrated regional attacks on U.S. Embassies or Businesses • Invasion or Loss of Major Ally or Partner • Regional Security Organization (NATO) breakup • Major epidemic or natural disaster (Spanish Flu of 1918, Katrina)	• Nuclear War (U.S. or Allies) • WMD Terror Attack • Domestic Rebellion • Pandemic or natural disaster that threaten U.S. existence
The Security of the U.S. economy and the global economic system	HLD/Vital Ally/Global Partner/Regional Other/Local	• 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 Int'l norms • U.S. Depression	• Financial failure of major institution or market • Major Degradation of critical infrastructure • Access to Global Domain(s) disrupted by adversary	• Global or U.S. economic collapse • Closed economic system • Destruction of critical infrastructure • Seizure of U.S. business/industry • Access to Global Domain(s) denied by adversary.
Preservation and extension of universal values	HLD/Vital Ally/Global Partner/Regional Other/Local	• Local Atrocities • Imposition of martial law by Ally or Partner • Democratic regression in Ally or Partner	• Mass atrocities • Democratic regression in Key Ally or Partner • Local imposition of alternate value system	• Genocide (Holocaust) • Regional imposition of alternate value system • Emergence or powerful totalitarian nation	• Global Imposition of alternative value system
Advancing and maintaining U.S. led International Order	HLD/Vital Ally/Global Partner/Regional Other/Local	• Local or State order undermined or replaced by alternative system, neutral or antagonistic to U.S. system (sets negative precedent)	• Regional Order undermined or replaced by alternative system, neutral or antagonistic to U.S. system	• Elements of International order undermined or replaced by alternative system, neutral or antagonistic to U.S. system	• U.S. Order Replaced in total by alternate system, hostile to current U.S. system

Figure 11. Military Strategic Risk Matrix – Consequence Development

(b) Once an assessor has determined levels of strategic value of interest and sources of risk using Figure 11, a consequence level can be assessed using Figure 12. This consequence will be paired with probability to assess risk level during risk judgement.

		Sources of Risk			
		Confined	**Considerable**	**Catastrophic**	**Existential**
Strategic Value of Interest	**HLD / Vital**	Modest	Major	Extreme	Extreme
	Ally / Global	Modest	Major	Major	Extreme
	Partner / Regional	Minor	Modest	Major	Major
	Other / Local	Minor	Minor	Modest	Modest

Figure 12. Military Strategic Risk Matrix – Consequence Assessment

(2) Military Risk. There are two categories of military risk: Risk-to-Mission (RM) and Risk-to-Force (RF). RM is the probability and consequence of current and contingency events causing harm to current or future military

objectives, while RF is the probability and consequence of current 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 JF Provider's ability to support CCMD missions. The concepts of RM and RF can be differentiated into four risk subsets based on source of risk and time horizon (Figure 13). Operational risk and future challenges risk measure RM, while force management risk and institutional risk measure RF. Time horizon will remain subjective based on strategic trends, threats, guidance provided by the CJCS and policy. Generally, the JF considers risk in relation to three time horizons: force employment (0–3 years), force development (2–7 years), and force design (5–15 years).

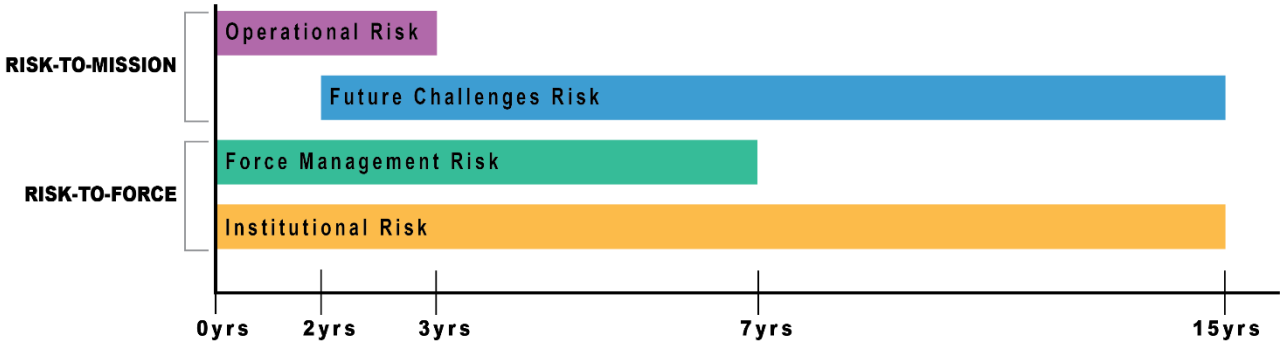

Figure 13. Military Risk Subsets

(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. It reflects the current force's ability to attain current 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 force employment period. The Time-Phased Force Deployment Data (TPFDD) for each of these plans serves to identify and limit risk to the force. Plans without a verified TPFDD have more risk. Commanders consider the feasibility of these plans in conjunction with operational concerns, such as the potential for escalation, to assess risk to a threat adequately.

2. Future challenges risk is a function of the probability and consequence of failure to meet future mission requirements. It reflects the future force's ability to achieve future mission objectives in the force development and force design periods, 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 current versus future risk in their 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 force employment and force development periods.

2. Institutional risk is a function of the probability and consequence of the DoD or Services 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 timeframe associated with this risk subset is much broader. All three time categories—force employment, force development, and force design—will impact institutional risk. It considers organization and process effectiveness, including the acquisition process, as well as program health, health of the force, and the defense industrial base.

(c) Military risk is assessed using the four probability levels and four consequence levels depicted in Figure 14. As with military strategic risk, judgment is required to integrate different levels of probability and consequence during Risk Characterization. Commanders and their staffs must place risk in context through the application of costs, impacts, time, and end-states.

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

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, Objective Achievable • RF, Joint Force Fully Sustained and Requirements Sourced

Figure 14. Military Risk Probability and Consequence Levels

1. Figure 15 provides an example of standard criteria across several variables to help frame the discussion on consequences. The Military Risk Matrix serves as a common risk framework for the GFM process across the JF, as directed in the Global Force Management Implementation Guidance (GFMIG). 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 JF. However, the risk analysis should not be limited to the metrics shown in Figure 15. If other metrics and categories present relevant information, they should be included in the analysis to facilitate leadership making the most informed decision possible. Commanders and staffs can reach a military risk assessment by coupling probability and consequence assessments during the risk judgement pillar.

Military Risk Subset	Reference	Risk Drivers Categories	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 provide 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
		DOTMLPF-P Capability vs. Threat Capability	Dominance	Superiority	Parity	Inferiority
Future Mission / Force	JFRR & DRRS	Readiness (DRRS)	Full spectrum C1 full capacity	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
	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	1:1.4>M2D≥1:3	M2D<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-Mcurdy)	Program failure, zeroed out (de-funded)
	JCIDS / AJA	Force Development & Design 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 imparatives (minor critical capability gaps)	Operational imperatives not achieved (major critical capability gaps)

Figure 15. Military Risk Matrix – Consequence Assessment

c. CRA Risk Judgement

(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 can be qualified as "Trending Up" or "Trending Down" based on a perceived direction of risk over time. While numerous senior officers, stakeholders, and experts contribute ideas and thoughts on how to characterize each risk, the CJCS makes the final decision on risk levels conveyed in the CRA.

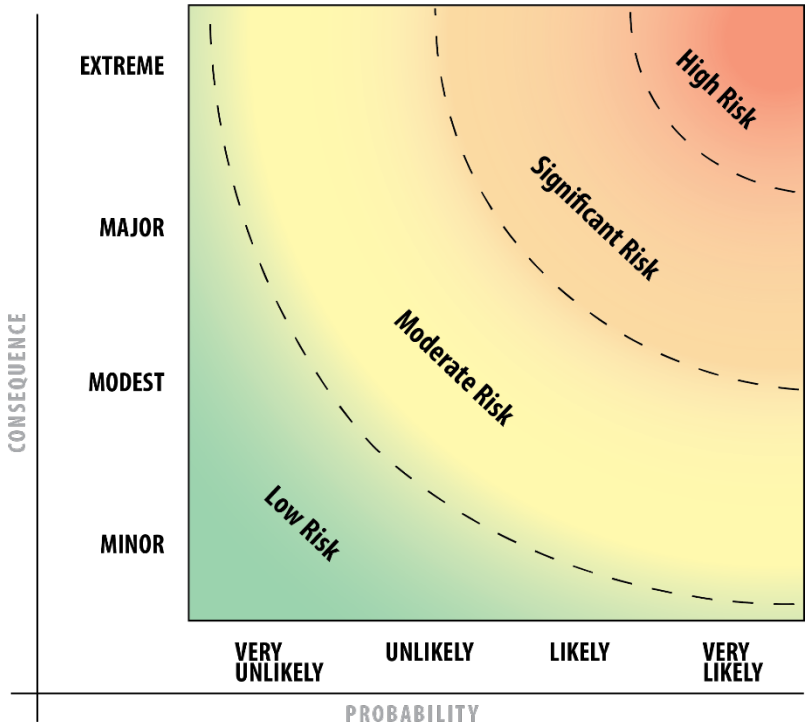

Figure 16. Military Strategic Risk and Military Risk Contour

(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 report and forwards it to the CJCS for signature. It is then passed to the SecDef to evaluate and manage the risk.

(2) CRA Risk Evaluation

(a) The SecDef determines the acceptability of risk presented in the CRA report and develops options for managing the risk. Depending on the situation, the SecDef may decide to accept, avoid, mitigate, or transfer the risk as described in Enclosure B, JRAM. For example, the SecDef may accept risk in the near-term, while directing mid-term mitigation actions or transferring risk to the future by focusing resources on current issues. In this case, transfer would be asking the next higher authority, the President, to decide to accept this risk.

(b) Another major consideration during risk evaluation is to trade space between military strategic risk and military risk. This is particularly true if an adversary acts in an opportunistic fashion. The key is to 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 (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 report. For example, Combatant Commanders and Service Chiefs must have a common understanding of terms, definitions, and how to characterize risk. This is necessary to properly convey risk in their Annual Joint Assessment (AJA) Survey responses, which provide significant 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.

3. Summary. The CRA serves as the keystone for risk calculation to the Nation's strategy and JF. Together with the NMS, the JF will use the CRA as a starting point to appraise risk for other processes and operations.

ENCLOSURE D

REFERENCES AND OTHER 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. *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 documents 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, "DoD Safety and Occupational Health (SOH) Program," October 14, 2014. 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 JF 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. *Global Force Management Implementation Guidance,* 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 to meet its Unified Command Plan-assigned Strategic Deterrence mission. RoSDF assesses the probability of an attack or series of attacks, regardless of means, that are intended to cause major or extreme consequences to U.S. national interests.

(INTENTIONALLY BLANK)

CJCSM 3105.01A
12 October 2021

GLOSSARY

PART I-ABBREVIATIONS AND ACRONYMS

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

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
GCP	Global Campaign Plan
GFM	Global Force Management
GFMIG	Global Force Management Implementation Guidance
IRGC	International Risk Governance Council
ISO	International Organization for Standardization
JF	Joint Force
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
SecDef	Secretary of Defense
TPFDD	Time-Phased Force Deployment Data

PART II-DEFINITIONS

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.

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 – There are two categories of military risk: Risk-to-Mission (RM) and Risk-to-Force (RF). RM is the probability and consequence of current and contingency events causing harm to current or future military objectives, while RF is the probability and consequence of current and contingency events causing harm to the provision and sustainment of sufficient military resources.

Military Strategic Risk – The probability and consequence of current and contingency events with direct military linkages upon the United States. This includes U.S. population, territory, civil society, institutional processes, critical infrastructure, and 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 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 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 – A component of the JRAM and also the fourth pillar, where risk decisions to accept, avoid, mitigate, or transfer risk are designed, implemented, and monitored.

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.

(INTENTIONALLY BLANK)