Working Paper

JAY ATANDA, MATTHEW NICOTRA, BENJAMIN SPERISEN, ELIKA SOMANI, HENRY H. WILLIS

# Living Framework and Guidelines for Information Disclosure in Biosecurity, Annex I

## Assessment Forms

RAND Global and Emerging Risks

WR-A4258-2
January 2026

RAND working papers are intended to share early insights and solicit informal peer review. This working paper has been approved for circulation by RAND but has not been peer reviewed or professionally edited or proofread. Feedback to the project team is welcome via email. This working paper can be quoted and cited without permission of the author, provided the source is clearly referred to as a working paper. This working paper does not necessarily reflect the opinions of RAND's research clients and sponsors. RAND® is a registered trademark. Learn more at www.rand.org.

For more information on this publication, visit **www.rand.org/t/WRA4258-1**.


### About RAND

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

### Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.



Published by the RAND Corporation, Santa Monica, Calif.


© 2026 RAND Corporation
RAND® is a registered trademark.

### Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, visit www.rand.org/about/publishing/permissions.



WR-A4258-2

# About This Annex

Advances in biological research can produce powerful insights with broad public benefits – but can also generate information that, if misused, poses serious biosecurity risks. Yet institutions lack clear, actionable guidance on how to assess and respond to such risks without stifling innovation or scientific discovery.

In response, RAND CAST has developed a living framework and toolkit to support responsible decisions about the disclosure of potentially hazardous biosecurity information. This framework is grounded in the principle that researchers and institutions must balance the societal benefits of open science with the real and growing risks of misuse of potentially dangerous information. It also provides a structured process for identifying when and how to pause, limit, or modify the release of sensitive research findings. Importantly, the framework is designed to be *simple*, *transparent*, *actionable*, *improvable,* and *repeatable* – capable of evolving as technologies change and our understanding of risk matures.

This annex provides blank assessment forms. The main working paper is available: www.rand.org/t/WRA4258-1

## RAND Center on AI, Security, and Technology

RAND Global and Emerging Risks is a division of RAND that delivers rigorous and objective public policy research on the most consequential challenges to civilization and global security. This work was undertaken by the division's Center on AI, Security, and Technology, which aims to examine the opportunities and risks of rapid technological change, focusing on artificial intelligence, security, and biotechnology. For more information, contact cast@rand.org.


## Funding

This research was independently initiated and conducted within the Center on AI, Security, and Technology using income from operations and gifts and grants from philanthropic supporters. The research was completed through funding provided by philanthropic supporter Coefficient Giving. A complete list of donors and funders is available at www.rand.org/CAST. RAND clients, donors, and grantors have no influence over research findings or recommendations.

# Contents

About This Annex ..... iii
Figures and Tables ..... v
Appendix C. Information Hazards ..... 1
Appendix D. Instructions ..... 4
Information Hazard Assessment: Part I ..... 5
Characterizing Risk Information ..... 5
Characterizing Benefits ..... 8
Information Hazard Assessment: Part II ..... 10
Characterizing Risk Information ..... 10
Likelihood of Risk ..... 14
Consequence Management ..... 16
Outcome Determination ..... 20
Nominal Scores ..... 20
Risk Scores ..... 20

# Figures and Tables

## Figures

Figure 1: Risk Groups, Outcomes and Mitigation Actions ..... 22

## Tables

Table 1: Likelihood Scores and Descriptions ..... 20
Table 2: Consequence Scores and Descriptions ..... 20
Table 3: Likelihood Risk Scores ..... 21
Table 4: Consequence Risk Scores ..... 21

# Appendix C. Information Hazards

An information hazard (IH) is a risk that arises from the dissemination or the potential dissemination of true information that may cause harm or enable some agent to cause harm.[1] Because most information could conceivably be used for benevolent or harmful purposes, it is useful to focus on those that are most worrying. As such, we define an information hazard of concern (IHC) as an IH which could be misapplied to do harm with no, or only minor, modification to pose a significant threat with broad potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security. Since IHC's are a subset of IH's, only some IH are an IHC. Note that the IHC definition is synonymous to the definition of dual use research of concern (DURC) as stated in United States government DURC; Potential Pandemic Pathogen Care and Oversight (P3CO); and Pathogens with Pandemic Potential (PPP) policies.[2]

---

[1] Bostrom, Nick, "Information Hazards: A Typology of Potential Harms from Knowledge," Review of Contemporary Philosophy, Vol. 10, 2011, pp. 44–79. As of January 21, 2026: https://nickbostrom.com/information-hazards.pdf

[2] There are six previous and one present U.S. government dual-use policies. They are as follows:
1) U.S. Government, *USG Policy for Oversight of Life Sciences DURC* (Federal DURC Policy), March 29, 2012. As of June 23, 2025: https://aspr.hhs.gov/S3/Documents/us-policy-durc-032812.pdf;

2) U.S. Government, *USG Policy for Institutional Oversight of Life Sciences DURC* (Institutional DURC Policy), September 24, 2014. As of June 23, 2025: https://osp.od.nih.gov/wp-content/uploads/United_States_Government_Policy_for_Institutional_Oversight_of_Life_Sciences_DURC.pdf;

3) Office of Science and Technology Policy, *Recommended Policy Guidance for Departmental Development of Review Mechanisms for Potential Pandemic Pathogen Care and Oversight* (P3CO), January 9, 2017. As of June 23, 2025: https://aspr.hhs.gov/S3/Documents/P3CO-FinalGuidanceStatement.pdf;

4) U.S. Department of Health and Human Services, *Framework for Guiding Funding Decisions about Proposed Research Involving Enhanced Potential Pandemic Pathogens* (HHS P3CO Framework), December 2017. As of June 23, 2025: https://aspr.hhs.gov/S3/Documents/P3CO.pdf;

5) U.S. Government, *USG Policy for Oversight of DURC and Pathogens with Enhanced Pandemic Potential* (DURC-PEPP Policy), May 6, 2024. As of June 23, 2025: https://aspr.hhs.gov/S3/Documents/USG-Policy-for-Oversight-of-DURC-and-PEPP-May2024-508.pdf;

6) U.S. Government, *Implementation Guidance / Implementation Plan for the DURC-PEPP Policy*, May 6, 2025. As of June 23, 2024: https://aspr.hhs.gov/S3/Documents/USG-DURC-PEPP-Implementation-Guidance-May2024-508.pdf.

7) White House, *Executive Order on Improving the Safety of Biological Research*, May 5, 2025. As of June 23, 2025: https://www.whitehouse.gov/presidential-actions/2025/05/improving-the-safety-and-security-of-biological-research/

This definition acknowledges the significant overlaps that exist between IH, IHC, dual use research (DUR) and DURC. For example, an information hazard could simultaneously be a DURC, the product of "life sciences research that, based on current understanding, can be reasonably anticipated to provide knowledge, *information*, products or technologies that could be misapplied to do harm with no, or only minor, modification to pose a significant threat with potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel or national security".[2]

These assessments focus *primarily* on research outcomes or actions that may result in *knowledge or information* products that could pose a hazard i.e. IH and IHC. As a secondary consideration, are research outcomes or actions that may result in knowledge, information, technologies, products, equipment or materials that also warrant careful assessment for DUR or as potential DURC, because of the overlap that exists with IH and IHC. The secondary considerations are research outcomes that we used as a guide for development of the assessment questions. These outcomes are defined by the National Science Advisory Board for Biosecurity (NSABB)[2] and U.S. government policies on DURC, P3CO, and PPP[3] that expands current and erstwhile narrow definitions of research categories as follows:

- From NSABB, the seven (7) categories of experiments:
  - I. Enhance the harmful consequences of the agent or toxin;
  - II. Disrupt immunity or the effectiveness of an immunization against the agent or toxin without clinical or agricultural justification;
  - III. Confer to the agent or toxin resistance to clinically or agriculturally useful prophylactic or therapeutic interventions against that agent or toxin or facilitates their ability to evade detection methodologies;
  - IV. Increase the stability, transmissibility, or the ability to disseminate the agent or toxin;
  - V. Alter the host range or tropism of the agent or toxin;
  - VI. Enhance the susceptibility of a host population to the agent or toxin; or
  - VII. Generate or reconstitute an eradicated or extinct agent or toxin listed in the policy.
- From U.S. government DURC, P3CO and PPP policies, Categories 1 and 2 research:
  - I. Category 1 research meets three criteria: (1) It involves one or more of the biological agents and toxins specified by the Federal Select Agents and Program; (2) It is reasonably anticipated to result, or does result, in one of the experimental outcomes listed in the NSABB seven categories of experiments above; and (3) Based on current understanding, the research constitutes DURC;

[3] National Science Advisory Board for Biosecurity, *Proposed Biosecurity Oversight Framework for the Future of Science*, March 2023. As of January 21, 2026: https://osp.od.nih.gov/wp-content/uploads/2023/03/NSABB-Final-Report-Proposed-Biosecurity-Oversight-Framework-for-the-Future-of-Science.pdf.

II. Category II research meets three criteria: (1) It involves, or is reasonably anticipated to result in a PPP;[4] (2) It is reasonably anticipated to result in, or does result in, one or more of the experimental outcomes listed below;[5] and (3) Based on current understanding, the research is reasonably anticipated to result in the development, use, or transfer of a PEPP[6] or an eradicated or extinct PPP that may pose a significant threat to public health, the capacity of health systems to function, or national security.

[4] A "pathogen with pandemic potential (PPP)" is a pathogen that is likely capable of wide and uncontrollable spread in a human population and would likely cause moderate to severe disease and/or mortality in humans.

[5] Category 2 experimental research outcomes or actions includes those reasonably anticipated to:

I. Enhance transmissibility of the pathogen in humans;
II. Enhance the virulence of the pathogen in humans;
III. Enhance the immune evasion of the pathogen in humans such as by modifying the pathogen to disrupt the effectiveness of pre-existing immunity via immunization or natural infection; or
IV. Generate, use, reconstitute, or transfer an eradicated or extinct PPP, or a previously identified PEPP.

[6] A "Pathogen with enhanced pandemic potential (PEPP)" is a type of PPP resulting from experiments that enhance a pathogen's transmissibility or virulence, or disrupt the effectiveness of pre-existing immunity, regardless of its progenitor agent, such that it may pose a significant threat to public health, the capacity of health systems to function, or national security.

## Appendix D. Instructions

The Part I form *must* be completed and submitted to Meselson Center management alongside your proposal, *pre-approval* i.e. *before your project starts*. Your answers in Part I should be short and succinct – you will potentially be expanding on them later in Part II.

The Part II form must be completed and submitted to MC management within 8 weeks of the project's start *but no later than the project midpoint*.

## Information Hazard Assessment: Part I

*Characterizing Risk Information*

Question 1.1

**Might this project discover previously unknown types of information hazards, create new instances of known information hazards, or add to or spread existing information hazards?**

*Choose one:*

- Yes
- Maybe
- No

🛑 If no, STOP assessment 🛑

*If you wish, provide a rationale for your choice in the text box (ideally 1-4 sentences)*

---

Question 1.2

**Describe *what* you are worried about discovering/creating/bringing attention to.**

- It's okay to be vague if this is just a speculative concern and you're not sure exactly what will be produced, or if you are worried that providing too much detail here would itself be a risk.
- If you leave information out or are intentionally vague because providing too much detail here would be a risk, let us know.

*Respond in the text box (ideally 1-4 sentences)*

---

Question 1.3

**Describe *why* you are worried about the information you shared in Question 1.2**

- In your response, consider the distinction between an "information hazard" and an "information hazard *of concern*".

*Respond in the text box (ideally 1-4 sentences)*

---

Question 1.4

**Describe any thoughts you have on *who* could misuse the information described in Question 1.2.**

- This question is designed to elicit information on the "who" – "who could misuse the information you have described in Q1.2" with a focus on actor sophistication and capabilities
- In responding consider skill level (e.g., layperson vs undergraduate biology major vs PhD level biologist), type (e.g., non-state vs state), and size (e.g., individual vs small group vs large group)

*Respond in the text box (ideally 1-4 sentences)*

---

Question 1.5

**Describe any thoughts you have on the *severity of the harm* that might arise from misuse the information described in Question 1.2**

- The following high-risk examples are a guide. In responding, research teams should also consider other *more nuanced examples of low/moderate risk*:
    - Morbidity (frequency of illness)
    - Mortality (frequency of death)
    - Results in outbreak, endemic/epidemic/pandemic event
    - Results in existential or catastrophic event

*Respond in the text box (ideally 1-4 sentences)*

---

Question 1.6

**Describe *how* your concerns in Question 1.2 could be mitigated.**

- Consider mitigation measures including (but not limited to):
    - Not conducting the research
    - Proceeding with only certain parts of the research
    - Limiting distribution of research results

*Respond in the text box (ideally 1-4 sentences)*

---

Question 1.7

**Describe *how* information or results generated in this project will be shared, including *who* will have access to the final product(s).**

*Respond in the text box (ideally 1-4 sentences)*

---

## *Characterizing Benefits*

Instructions: Answer Questions 1.8 to 1.10 to the best of your ability. Short answers are acceptable for Q1.10 – Meselson Center management will conduct a more detailed benefits analysis.

- In your response to Q1.10, consider beneficial purposes that could be served by the generated information other than in countering or responding to the very harm that the information could cause. In other words, what benefits are lost (beyond just ameliorating harm) by restrictions on the widespread availability of the information?

Question 1.8

**Science-centric benefits (indicate one or more):**

a. Could the research provide critical insights into viral transmission? (Yes / No / DK)
b. Could the research provide insights into development of vaccines? (Yes / No / DK)
c. Could the research provide insights into development of therapeutics? (Yes / No / DK)
d. Could the research provide insights into development of diagnostics? (Yes / No / DK)
e. Could the research support development of improved countermeasures? (Yes / No / DK)
f. Could the research support improved disease surveillance? (Yes / No / DK)
g. Other benefits (Describe in Q1.10) (Yes / No / DK)

Question 1.9

**Policy-centric benefits (indicate one or more):**

a. Could the research enhance biosecurity? (Yes / No / DK)
b. Could the research support prevention of accidental releases? (Yes / No / DK)
c. Could the research support prevention of intentional releases? (Yes / No / DK)
d. Could the research support public health preparedness? (Yes / No / DK)
e. Could the research support international security cooperation? (Yes / No / DK)
f. Other benefits (Describe in Q1.10) (Yes / No / DK)

Question 1.10

**Describe any other benefits of your project in 1-2 sentences.**

Provide a few short sentences – not more than one paragraph describing the benefits and advantages of the information your project will generate.

*Respond in the text box (ideally 1-4 sentences)*

## Information Hazard Assessment: Part II

### *Characterizing Risk Information*

Instructions: Questions 2.1 to 2.6 provide information characterizing the nature of the risk. If your answers to a question remains unchanged from Part I, restate or copy/paste the prior response.

#### Question 2.1

**Describe *how* the information you are concerned about could be used to cause harm?**

- In responding to this question, think about "courses of action" that could result in misuse of the information you generate, for example:
  - Could the information you generate be misused directly? Could the misuse occur when combined with existing information, whether publicly available or restricted?
  - For your consideration, other ways information could lead to harm include: *1)* For enabling a malefactor to develop a more effective weapon than they otherwise might be able to, *2)* For lowering the barriers to the development of a weapon, *3)* For evading detection of a weapon program, detection of a release, or attribution of an attack, and *4)* For impeding response to an attack.
- Consider the type of harm that could result from misuse of the information you generate. Examples of types of harm include those related to public health and safety, national security and critical infrastructure, food security, environmental impacts, economic impacts etc.

*Respond in the text box (ideally 1-4 sentences)*

---

🛑 If your project generates no potentially hazardous information, STOP assessment 🛑

Question 2.2

**How *novel* is the potentially hazardous information?**

- This question focuses on novelty of information generated i.e. "level of newness" of the information you generated. For example, on a sliding scale from "not very novel" to "novel" to "very novel"; compiling a list of nucleic acid synthesis companies that do not screen orders would not be very novel, compiling a list of genes that could plausibly be genetically engineered into an influenza virus to increase transmissibility 100x would be novel, while uncovering an entirely new threat (e.g. mirror life) would be considered very novel.

*Respond in the text box (ideally 1-4 sentences)*

---

Question 2.3

**Is the potentially hazardous information generated, also available through alternate, proxy sources, public or otherwise?**

- In this question, we would like to determine if the information you have generated is available via other sources public or otherwise. We describe these sources as alternate or proxy sources and ask research teams to consider peer reviewed, grey, and other open sources of information in their response.

*Choose one:*

- Yes
- Maybe
- No

*If Yes/Maybe describe in the text box (ideally 1-4 sentences)*

---

Question 2.4

**How *novel* is the *potential harm* that might be enabled by the information?**

- In your response, focus on "*novelty of potential harm*".
- Note distinction between this (novelty of potential harm) and Q2.2 (novelty of information). Here, we ask research teams to focus on novelty of the potential harm that could result if the information generated is misused.
- A response of "not applicable" or "don't know" is acceptable.
- If research teams think potential harms are not novel or have been adequately covered in 2.1, indicate so.

*Respond in the text box (ideally 1-4 sentences)*

Question 2.5

**If it is possible to characterize the *magnitude of harm* i.e. *quantify the harm* (described in Q1.5 and Q2.1) associated with misuse of the generated information, what would it be??**

- This might be hard to answer. We are looking for your best guesstimate of the information you have already provided in Questions 1.4 and 2.1.
- In your response, consider the following:
  - Morbidity (frequency of illness)
  - Mortality (frequency of death)
  - Results in outbreak, endemic/epidemic/pandemic event
  - Results in existential or catastrophic event

*Respond in the text box (ideally 1-4 sentences)*

Question 2.6

***Who* would be able to exploit this information to do harm, and *what* resources would be required??**

- Note that this question is two-part. The first is focused on eliciting information on the "*who*" – "who could misuse the information you have described in Q1.2" – Your answers to Q1.4 can be copied here. The second focuses on "*resources*" – what resources would be required to exploit the information generated to do harm.
- In your response, consider the following:
  - Ease of misuse
  - Actor type and size (state vs. non-state),
  - Potential actor abilities [general public (unskilled) vs science novice (college level/low-skilled) vs science expert (highly skilled/PhD-level)],
  - Access to infrastructure, equipment and money etc.

*Respond in the text box (ideally 1-4 sentences)*

*Likelihood of Risk*

Instructions: Questions 2.7 to 2.10 address the "likelihood of risk" using probability ranges. Choose one as your best guess and include a few clarifying sentences supporting your choice if you wish.

Question 2.7

**In your opinion, how likely is it that the project will generate this information?**
*Choose one:*

- Almost no chance/very unlikely (01-19%)
- Unlikely (20-44%),
- Roughly even chance (45-55%)
- Likely (56-80%)
- Very likely/almost certainly (81-99%)

*If you wish, provide a rationale for your choice in the text box (ideally 1-4 sentences)*

---

---

Question 2.8

**In your opinion, how likely is it that the information generated would actually be useful in generating the potential harms described above (Questions 2.1 and 2.5)?**
*Choose one:*

- Almost no chance/very unlikely (01-19%)
- Unlikely (20-44%),
- Roughly even chance (45-55%)
- Likely (56-80%)
- Very likely/almost certainly (81-99%)

*If you wish, provide a rationale for your choice in the text box (ideally 1-4 sentences)*

---

---

Question 2.9

**How confident are you that the potential harms described in Questions 2.1 and 2.5 could be successfully implemented? (Use assumptions about the existence, capabilities, intent and resources potentially malicious actors might need – see your response to Q2.6)**

*Choose one:*

- Almost no chance/very unlikely (01-19%)
- Unlikely (20-44%),
- Roughly even chance (45-55%)
- Likely (56-80%)
- Very likely/almost certainly (81-99%)

*If you wish, provide a rationale for your choice in the text box (ideally 1-4 sentences)*

---

Question 2.10

**How imminent would be the misuse of the generated information? (Use assumptions about the existence, capabilities, intent and resources potentially malicious actors might need – see your response to Q2.6)**

*Choose one:*

- Almost no chance/very unlikely (01-19%)
- Unlikely (20-44%),
- Roughly even chance (45-55%)
- Likely (56-80%)
- Very likely/almost certainly (81-99%)

*If you wish, provide a rationale for your choice in the text box (ideally 1-4 sentences)*

---

*Consequence Management*

Instructions: Questions 2.11 to 2.16 address "consequence management". Answer them to the best of your ability. Very short answers or "I don't know" are acceptable. Meselson Center management will conduct a more detailed analysis of consequence management.

Question 2.11

**Is the information generated export controlled (or would be if the government were aware of it)?**

- There are government export controls on certain types of nonpublic information or technical knowhow, that relate to U.S. export controls on semiconductors to China, control of the export of defense-related technical data under ITAR and EAR, export controls on select agents and toxins under FSAP etc.
- In your response, consider if your generated information will or already falls under these, or would potentially be export controlled if the government were aware of it (assuming this is wholly novel information)

*Choose one:*

- Yes
- Maybe
- Don't know
- No

*If Yes/Maybe describe in the text box (ideally 1-4 sentences)*

Question 2.12

**Could the information generated be useful for mitigation efforts (e.g. countermeasures development, better law enforcement etc.) against some of the potential harms described in Questions 2.1 and 2.5?**

- Your response should focus on ways your generated information can be used in driving mitigation efforts such as countermeasures development, better law enforcement etc.

*Choose one:*

- Yes
- Maybe
- Don't know
- No

*If Yes/Maybe describe in the text box (ideally 1-4 sentences)*

Question 2.13

**Ability to deter and prevent misuse (of the information)**

- Your response should focus on current abilities to deter and prevent misuse of your generated information. For example:
  - Deterring or preventing hazardous information misuse requires an integrated approach that includes physical protection, access controls, materials accountability, and personnel screening. Think about current capabilities related to these in your response.
  - Consider the effects of controlling access to this information: public information release (unencumbered and no restrictions) vs release to select audience on need-to-know basis (access control) or classification.
  - Screenings for reagents or equipment that are the rate limiting step in a pipeline; "know-your-customer" screenings for purchases of synthetic nucleic acids and benchtop nucleic acid synthesis equipment as an example.

*Respond in the text box (ideally 1-4 sentences)*

---

Question 2.14

**Ability to recognize misuse (of information) has occurred, or ability to recognize interest in misuse (of information)**

- Your response should focus on *current abilities* (typically government driven) *to identify* WHEN hazardous information has been misused

*Respond in the text box (ideally 1-4 sentences)*

---

Question 2.15

**Ability to attribute misuse that occurred**

- Your response should focus on current abilities (typically government driven) to determine WHO has misused hazardous information.

*Respond in the text box (ideally 1-4 sentences)*

Question 2.16

**Ability to provide for consequence management and recovery**

- Post-event consequence management includes response and recovery operations. In your response, focus on **CHANGES** to current ability to respond and recover from harm due to misuse or release of your generated information. For example, has/will the misuse or release of your generated information improve or decrease our ability to respond to the harms you have previously described (Questions 2.1 and 2.5)?
- Also consider changes to the following:
  - Coordination between enforcement and regulatory agencies
  - Actions focused on responding to harms described in Questions 2.1 and 2.5
  - Ability to make an initial characterization (Questions 2.1 to 2.5)
  - Ability to formulate initial protective actions and recommendations
  - Ability to conduct initial impact assessments, provide medical countermeasures and share incident-related information

*Respond in the text box (ideally 1-4 sentences)*

## Outcome Determination

### *Nominal Scores*

**Table 1: Likelihood Scores and Descriptions**

| Scores, Description and Probability Ranges | | |
|---|---|---|
| **Nominal Scores** | **Description** | **Reference Probability Range** |
| 1 | Almost no chance/very unlikely | 01-19% |
| 2 | Unlikely | 20-44% |
| 3 | Roughly even chance | 45-55% |
| 4 | Likely | 56-80% |
| 5 | Very likely/almost certainly | 80-99% |

**Table 2: Consequence Scores and Descriptions**

| Scores, Description and Operational Definitions | | |
|---|---|---|
| **Nominal Scores** | **Description** | **Operational/Mission Effects** |
| 1 | Negligible impact | No measurable loss of capability; routine functions continue. |
| 2 | Minor impact | Localized, short-term performance dip; work-arounds available. |
| 3 | Moderate impact | Noticeable degradation of one business line or region; recovery within weeks. |
| 4 | Major impact | Core mission cannot meet demand in most of the organization; months of recovery. |
| 5 | Catastrophic impact | System-wide failure; mission goals unmet anywhere; long-term recovery/irreversible loss. |

### *Risk Scores*

**Instructions for deriving risk scores:**

- Score from 1 to 5 (in **Tables 3 and 4**) using the nominal scales in **Tables 1 and 2**.
- Calculate average scores.
- Derive "anchored" scores.
- Annex II provides a *spreadsheet toolkit* to speed up this process.

**Table 3: Likelihood Risk Scores**

| | Scores/Rating, 1-5 |
|---|---|
| **Dimensions** | **Sliding nominal scoring scale from 1 to 5, representing lower risk to high+ risk. (*Score of 1 is lower risk. Score of 5 is high+ risk*)** |
| How likely is it that the project will generate hazardous information? | |
| How likely is it that the information generated would actually be useful in generating the harm(s) described above? | |
| How confident are you that the harm described above could be successfully implemented? | |
| How imminent is the misuse of the generated information? | |
| **Likelihood Score (Average) –** *Add scores and divide by 4* | |
| ***Anchored* Likelihood Risk Score**[a] | |

NOTE: Dimensions for "likelihood risk scores" are from Part II of the assessments – see Questions 2.7 to 2.10.
[a] Anchored Likelihood Risk Score derived as follows: 0 to 1: 1 >1 to 2: 2. >2 to 3: 3 >3-4: 4 >4 to 5: 5

**Table 4: Consequence Risk Scores**

| | Scores/Ratings, 1-5 |
|---|---|
| **Dimensions** | **Sliding nominal scoring scale from 1 to 5, representing negligible to catastrophic impact.** |
| Ability to deter and prevent misuse (of the information) | |
| Ability to recognize misuse (of the information) has occurred | |
| Ability to attribute misuse that occurred | |
| Ability to provide for consequence management & recovery | |
| **Consequence Score (Average) –** *Add scores and divide by 4* | |
| ***Anchored* Consequence Risk Score**[a] | |

NOTE: Dimensions for "consequence risk scores" are from Part II of the assessments – see Questions 2.13 to 2.16.
[a] Anchored Consequence Risk Score derived as follows: 0 to 1: 1 >1 to 2: 2. >2 to 3: 3 >3-4: 4 >4 to 5: 5

Risk Groups

**Instructions for deriving risk scores:**

- Match anchored scores from **Tables 3 and 4** to the appropriate risk group using **Figure 1**.
- Match color-coded risk group to outcome level and recommendation in **Figure 1**.
- If the spreadsheet toolkit (see ancillary files) is utilized, this process is all automated.
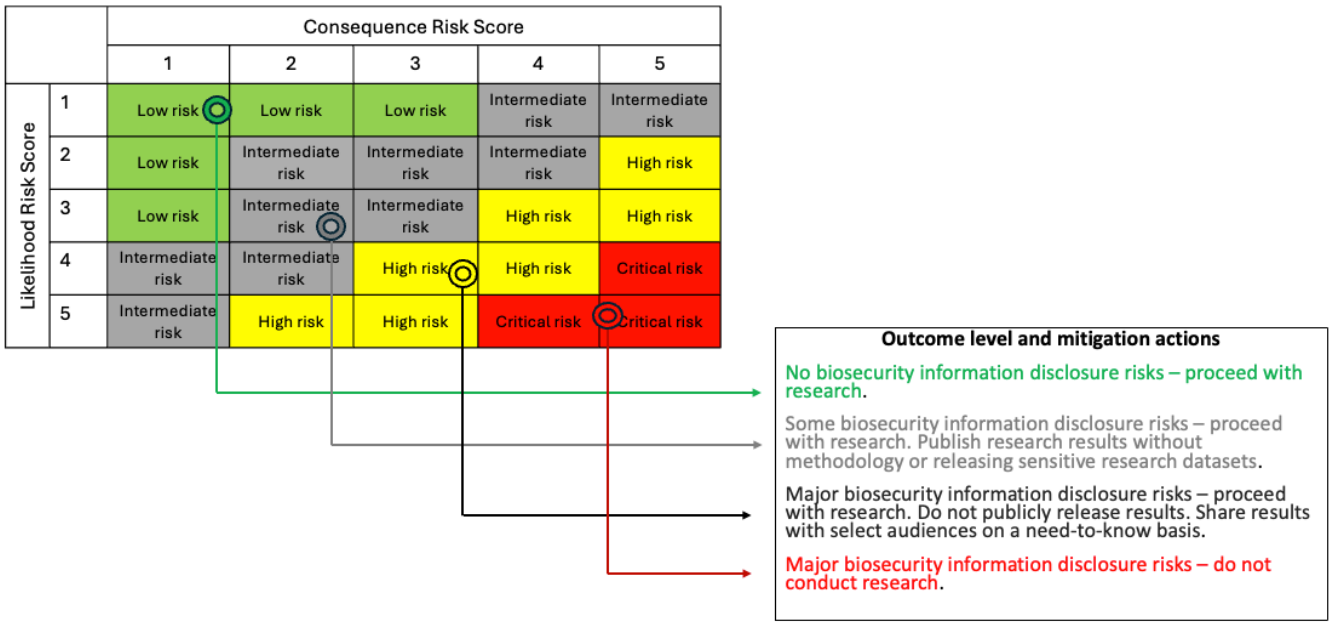
**Figure 1: Risk Groups, Outcomes and Mitigation Actions**