OPSEC Analysis Resources

Threat Assessment Worksheet

Who is the adversary?		
What is the adversary's objective?		
What is the adversary's intent?		
Does the adversary have friends? □ Yes □ No	**List the friends:**	A. ______________________________ B. ______________________________ C. ______________________________ D. ______________________________

Method	Intent	Capability	Threat Rating	**Proven:** Include Report # **Estimated:** Based on current intel
SIGINT				□ Proven □ Estimated
HUMINT				□ Proven □ Estimated
OSINT				□ Proven □ Estimated
GEOINT				□ Proven □ Estimated
MASINT				□ Proven □ Estimated

Friend A: ____

Method	Intent	Capability	Threat Rating	**Proven:** Include Report # **Estimated:** Based on current intel
SIGINT				□ Proven □ Estimated
HUMINT				□ Proven □ Estimated
OSINT				□ Proven □ Estimated
GEOINT				□ Proven □ Estimated
MASINT				□ Proven □ Estimated

Intent
High: Highly motivated
Med High: Significantly motivated
Medium: Sufficiently motivated
Med Low: Moderately motivated
Low: Not motivated

Capability
High: Optimal collection assets
Med High: Significant collection assets
Medium: Probable collection assets
Med Low: Possible collection assets
Low: Undeveloped collection assets

Critical Information & Indicators Worksheet

Based on your organization, mission, and threats, determine what items the complete CIL/CIIL might contain.

Who is the adversary?	
What is the adversary's objective?	
What strategy might the adversary employ?	

Critical Information Lists/Critical Information & Indicators List CIL/CIIL

Friendly CIL	**Adversary CIL**
What information is important to ensuring the success of your mission?	What information does the adversary need to achieve their goals?
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.
6.	6.
7.	7.

Combined CIL/CIIL

Critical Information Item	**Impact Rating**
1.	
2.	
3.	
4.	
5.	
6.	
7.	

Vulnerability Worksheet

Based on your organization, mission, and threats, determine what your top vulnerabilities.

Vulnerability	Assigned Rating
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Risk Analysis Worksheet

Use the information from the threat, critical information, and vulnerability worksheets to populate this risk analysis worksheet and calculate the overall risk to your organization.

#	Vulnerability	Rating
1		
2		
3		
4		
5		

Threat	Rating

#	Critical Info.	Rating
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Risk = Vulnerability × Threat × Impact

Probability = Vulnerability × Threat

Risk = Probability × Impact

Risk Analysis Summary Form							Acceptable Risk Level:__________		
Vul #	Vulnerability Rating	Threat Category	Threat Rating	Probability (V × T)	CI #	Critical Info. Impact Rating	Overall Risk	Counter-measures	Residual Risk

Countermeasures Worksheet

Part A

Based on the Risk Analysis chart you completed and what you have learned about vulnerabilities and countermeasures, come up with five possible countermeasures that will reduce the risk of your critical information being exploited or compromised.

Countermeasures
1.
2.
3.
4.
5.

Part B

- In the *Vulnerability* column, list each vulnerability in the *Risk Analysis Worksheet* that resulted in an overall risk that was *higher* than the Acceptable Level of Risk.
- In the *Original Vulnerability Rating* column, list the original rating for the vulnerability.
- In the *Countermeasure* column, indicate which countermeasure(s) might mitigate the vulnerability listed in the Original Vulnerability Rating column.
- In the *New Vulnerability Rating* column, identify what the new rating would be as a result of implementing the countermeasure.

Vulnerability	Original Vulnerability Rating	Countermeasure	New Vulnerability Rating
1.			
2.			
3.			
4.			

Part C

Complete the *Risk Analysis Summary Form* on the next page and calculate the *Residual Risk* rating that would occur if the countermeasures are implemented.

- The *New Vulnerability Rating* value from Part B should be listed in the *Vulnerability Rating* column.
- Remember that the rating values for Threat and Critical Information Impact do not change.

Risk Analysis Summary Form							Acceptable Risk Level:		
Vul #	Vulnerability Rating	Threat Category	Threat Rating	Probability (V × T)	CI #	Crit. Info. Impact Rating	Overall Risk	Counter-measures	Residual Risk
1									
2									
3									
4									
5									
6									
7									
8									

Resources Section

Standard Threat Rating Matrix

Standard Critical Information (Impact) Rating Matrix

Standard Vulnerability Rating Table

Standard Probability Matrix

Standard Risk Assessment Rating Matrix

OPSEC Process Flow Chart for Risk Analysis

Standard Threat Rating Matrix

This matrix uses percentages because threat is a probability factor.

Intent (%) × Capability (%) = Threat (%)		Estimated Adversary Capability				
		High	**Med High**	**Medium**	**Med Low**	**Low**
		Highly developed and most likely in place OR the adversary receives equivalent data from a highly capable third party.	**Significantly developed** and probably in place OR the adversary receives equivalent data from a significantly capable third party.	**Possibly developed** and likely in place OR the adversary receives equivalent data from a capable third party.	**Probably not developed** and most likely not in place OR the adversary may receive equivalent data from a third party.	**Not developed** or does not receive data from a third party.
Estimated Adversary Intent	**High** The adversary is **highly motivated** and a successful outcome significantly contributes to meeting adversary objectives.	High	Med High	Medium	Med Low	Low
	Med High The adversary is **significantly motivated** and a successful outcome greatly contributes to meeting adversary objectives.	Med High	Medium	Medium	Med Low	Low
	Medium The adversary is **sufficiently motivated** and a successful outcome will contribute to meeting adversary objectives.	Medium	Medium	Med Low	Low	Low
	Med Low The adversary is **moderately motivated** and a successful outcome can contribute to meeting adversary objectives.	Med Low	Med Low	Low	Low	Low
	Low The adversary is **not motivated** to collect information.	Low	Low	Low	Low	Low

Standard Critical Information (Impact) Rating Matrix

This matrix requires converting the resulting percentage into a whole number because overall impact is not a probability factor.

		Estimated Impact of Loss of Critical Information				
	Importance of CI to Adversary (%) × Estimated Impact of Loss of CI (%) = Overall Impact (% × 100 = #)	**High**	**Med High**	**Medium**	**Med Low**	**Low**
		Loss of CI will have a **severe** impact on the ability to accomplish the mission	Loss of CI will probably have a **serious** impact on the ability to accomplish the mission.	Loss of CI will likely have an **appreciable** impact on the ability to accomplish the mission.	Loss of CI may have a **moderate** impact on the ability to accomplish the mission.	Loss of CI may have a **minor** impact on the ability to accomplish the mission.
Estimated Importance of CI to Adversary	**High** Of **critical** importance to the adversary. Obtaining the CI considerably contributes to meeting adversary objectives.	High	Med High	Medium	Med Low	Low
	Med High Of **crucial** importance to the adversary. Obtaining the CI appreciably contributes to meeting adversary objectives.	Med High	Medium	Medium	Med Low	Low
	Medium Of **essential** importance to the adversary. Obtaining the CI greatly contributes to meeting adversary objectives.	Medium	Medium	Med Low	Low	Low
	Med Low Of **moderate** importance to the adversary. Obtaining the CI somewhat contributes to meeting adversary objectives.	Med Low	Med Low	Low	Low	Low
	Low Of **minor** importance to the adversary. Obtaining the CI is a negligible contribution to meeting adversary objectives.	Low	Low	Low	Low	Low

Standard Vulnerability Rating Table

This chart uses percentages because vulnerability is a probability factor.

Rating (%)	Vulnerability Description
High	The adversary's capability to exploit the vulnerability is highly developed. They can exploit the vulnerability virtually any time. They can use at least one intelligence collection discipline to collect critical information.
Medium High	The adversary's capability to exploit the vulnerability is significantly developed. They can exploit the vulnerability most of the time. They can use at least one intelligence collection discipline to collect critical information.
Medium	The adversary's capability to exploit the vulnerability is somewhat developed. They can exploit the vulnerability some of the time. They may be able to use at least one intelligence collection discipline to collect critical information.
Medium Low	The adversary's capability to exploit the vulnerability is not well developed. They can exploit the vulnerability only occasionally. They may be able to use at least one intelligence collection discipline to collect critical information.
Low	The adversary has very limited capability to exploit the vulnerability. They are unable to exploit the vulnerability on a regular or on-demand basis.

Standard Probability Matrix

Probability is a percentage, so both the threat and vulnerability values are displayed as percentages.

- The estimated vulnerability rating is the category you selected from the Vulnerability chart.
- The calculated threat rating is the outcome from the Threat matrix when you multiplied intent and capability.

	Threat (%) × Vulnerability (%) = Probability (%)	**Calculated Threat Rating**				
		High	**Med High**	**Medium**	**Med Low**	**Low**
Estimated Vulnerability Rating	**High**	High	Med High	Medium	Med Low	Low
	Med High	Med High	Medium	Medium	Med Low	Low
	Medium	Medium	Medium	Med Low	Low	Low
	Med Low	Med Low	Med Low	Low	Low	Low
	Low	Low	Low	Low	Low	Low

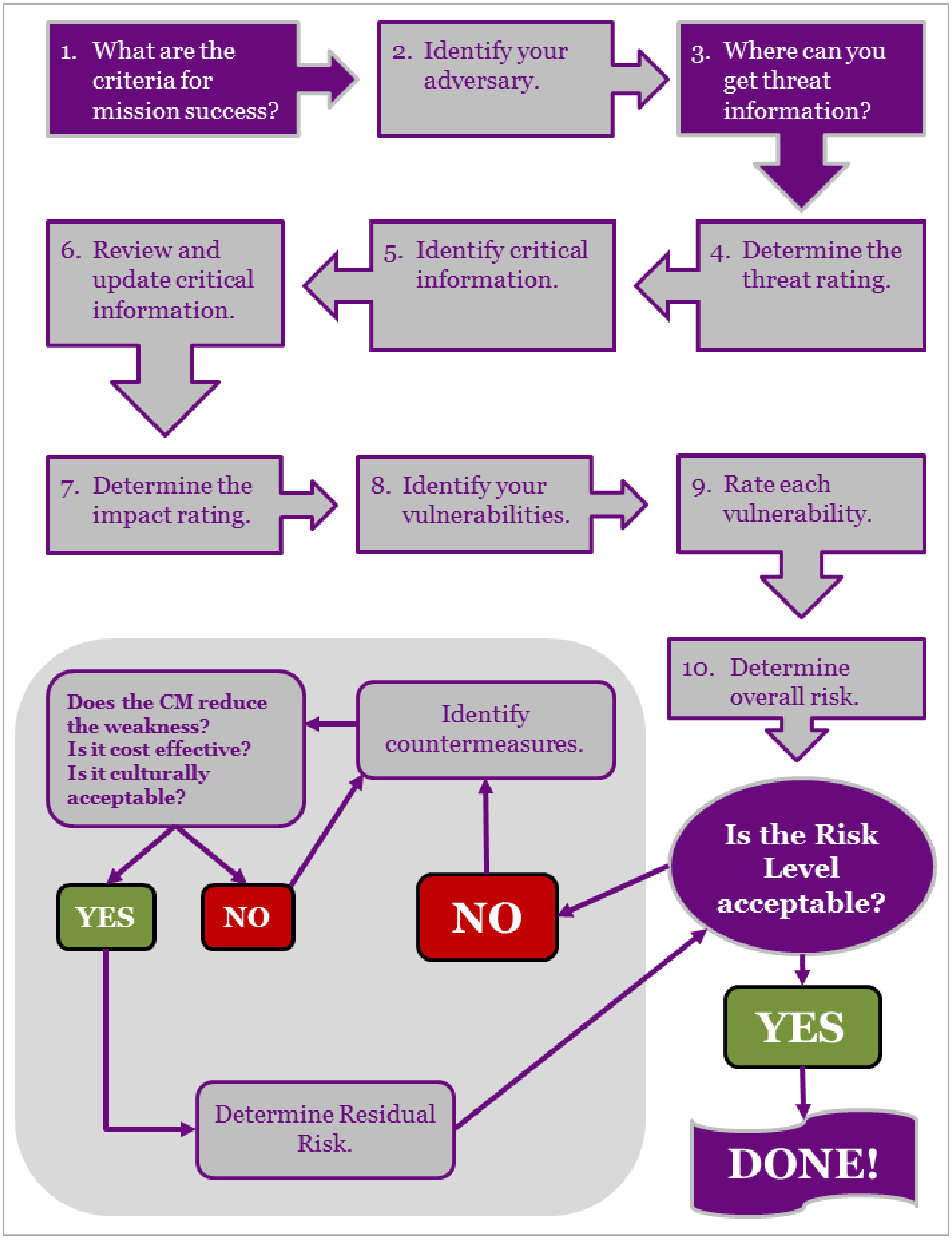
Standard Risk Assessment Rating Matrix

When estimating risk using the standard matrix, remember that probability is a percentage and impact is a whole number. The overall risk value is a whole number.

- The calculated probability rating is the outcome from the Probability matrix when you multiplied your threat and vulnerability values.
- The calculated impact rating is the outcome from the Critical Information matrix when you multiplied the CI's importance to the adversary and the CI's impact on your mission.

		Calculated Impact Rating (#)				
	Probability (%) × Impact (#) = Risk (#)	**High**	**Med High**	**Medium**	**Med Low**	**Low**
Calculated Probability Rating (%)	**High**	High	Med High	Medium	Med Low	Low
	Med High	Med High	Medium	Medium	Med Low	Low
	Medium	Medium	Medium	Med Low	Low	Low
	Med Low	Med Low	Med Low	Low	Low	Low
	Low	Low	Low	Low	Low	Low

OPSEC Process Flow Chart for Risk Analysis


1. What are the criteria for mission success?
2. Identify your adversary.
3. Where can you get threat information?
4. Determine the threat rating.
5. Identify critical information.
6. Review and update critical information.
7. Determine the impact rating.
8. Identify your vulnerabilities.
9. Rate each vulnerability.
10. Determine overall risk.
Is the Risk Level acceptable?
YES
DONE!
NO
Identify countermeasures.
Does the CM reduce the weakness? Is it cost effective? Is it culturally acceptable?
YES
NO
Determine Residual Risk.

NOTES: