This document was exported from Numbers. Each table was converted to an Excel worksheet. All other objects on each Numbers sheet were placed on separate worksheets. Please be aware that formula calculations may differ in Excel.

Numbers Sheet Name	Numbers Table Name	Excel Worksheet Name
RAR of NC Security Controls		
	Table 1	RAR of NC Security Controls
RAR Instructions		
	Table 1	RAR Instructions
RAR Likelihood & Risk Matrices		
	Table 1	RAR Likelihood & Risk Matrices
RAR Executive Summary		
	Table 1	RAR Executive Summary

DoD Risk Assessment Report (RAR) of Non-Compliant (NC) Security Controls

(1) System Name	(2) System Acronym	(3) DoD Component	(4) System Identification	(5) System Type
Initrobe	Init15	*AF*	**Lab 3**	*Lab 3*

(6) Authorizing Official	(8) Authorization Status	(9) Assessment Completion Date	(10) Period Covered: Authorization Date	(10) Period Covered: Authorization Termination Date	(11) Last Update
Someguy Namedoug	*Fully*	1.10.2024	**1.09.2024**	**1.11.2024**	**1.10.2024**

(7) Security Controls Assessor (SCA) and/or SCA Representative	(12) System Categorization: Confidentiality	Integrity	Availability
These Guys	*SHHHHHHH*	*LOTS*	*MINIMAL*

(13) Stakeholder Information	
ISO:	1500
ISSM:	NONE
Other:	YES

(14) Executive Summary: SUMMARIS EXECUTIVUS MYSTERIOUS

(15) Summary of Risk Assessment Results:

(15a) Risk Determination

Likelihood	Impact: Very Low	Low	Moderate	High	Very High
Very High				*I*	*C,A*
High					
Moderate					
Low					
Very Low					

Legend
Very High
High
Moderate
Low
Very Low

(15b) Non-Compliant Security Controls by Risk Level *(Before Mitigation)*

Security Objectives	Impact: Very Low	Low	Moderate	High	Very High
	2	*3*	*6*	*4*	*2*

(15c) Non-Compliant Security Controls by Risk Level *(After Proposed Mitigation)*

Security Objectives	Impact: Very Low	Low	Moderate	High	Very High
	5	8	4	0	0

(16) Specific Vulnerabilities

Non-Compliant Security Controls (16a)	Vulnerability Description *(From SAR)* (16b)	Security Objectives *(C-I-A)* (16c)	Severity or Pervasiveness *(VL-VH)* (16d)	Relevance of Threat *(VL - VH)* (16e)	Likelihood (Cells 16d & 16f) *(VL - VH)* (16f)	Impact *(VL - VH)* (16g)	Impact Description (16h)	Risk (Cells 16f & 16g) *(VL -VH)* (16i)	Proposed Mitigations *(From POA&M)* (16j)	Residual Risk *(After Proposed Mitigations)* (16k)	Recommendations (16l)
	MikroTik RouterOS < 6.41.3		VH	VH	VH	VL	remote attack	VH	upgrade router OS	low	
	MikroTik RouterOS HTTP		VH	VH	VH	VL	remote attack	VH	upgrade router OS	low	
	libupnp < 1.6.18		VH	VH	VH	VL	remote attack	VH	upgrade libupnp > 1.6.18	low	

DoD Risk Assessment Report of Non-Compliant (NC) Security Controls Instructions

Please find below instructions for completing the DoD Risk Assessment Report of non-compliant security controls. The report is to communicate risk assessment results to organizational decision makers to support risk responses. This report also addresses vulnerabilities displayed in the SAR after the security control assessment has been completed by the SCA. All NC security controls must be subjected to a risk assessment that considers multiple factors in assigning a residual risk level to each NC security control. The individual risk levels are then used to inform the SCA's recommendation (i.e., SAR executive summary) to the Authorizing Official on acceptance of the cybersecurity risk of operating the system.

Item #	Field Name		Field Description/Instructions
	Header		
1	System Name		Full descriptive name of the system and system version number. *Example: Agency Billing System* ***Information can be obtained from the Security Plan (System Name).***
2	Acronym		Provide a shortened or commonly used name or abbreviation (upper case) for the system name. Example: ABS ***Information can be obtained from the Security Plan (Acronym).***
3	DoD Component		Parent or governing Component that manages, owns, and/or controls the system. Select from the drop down box the correct DoD Component, Combatant Command, Service, or Agency that owns the IS or PIT system. *Drop Down List to include all CC/S/As* ***Information can be obtained from the Security Plan (DoD Component).***
4	System Identification		Unique system identifier (typically a number or code) used by the DoD Component to uniquely identify the system. This is usually the DITPR ID. *Example: 63221* ***Information can be obtained from the Security Plan (System Identification).***
5	System Type		Identify the DoD information system type. *Drop Down:* *IS Major Application* *IS Enclave* *Platform IT System* ***Information can be obtained from the Security Plan (System Type).***
6	Authorizing Official (AO)		The name of AO for whom the RAR was prepared. ***Information can be obtained from the Security Plan (RMF POCs, Member Names, and Contact Information Table).***
7	SCA or SCA Representative		The name of the individual serving as the Security Controls Assessor (SCA) or SCA Representative for the system. ***Information can be obtained from the Security Plan (RMF POCs, Member Names, and Contact Information Table).***
8	Authorization Status		*Choose from the drop down list the authorization decision for the information system:* *Not yet authorized* *ATO* *ATO with Conditions* *IATT* *DATO* ***Information can be obtained from the Security Plan (Authorization Status).***
9	Assessment Completion Date		List the date the security control assessment of the system was completed.
10	Period Covered		If the system is/was authorized, list the authorization date and the authorization termination date (ATD), even if they have expired. Example: Authorization Date: 23-Sep-05 ATD: 23-Sep-07 ***Information can be obtained from the SAR (Period Covered).***
11	Last Update		List the date of the last change that occurred on the security assessment report. This is primarily driven by updates to the security controls and their associated status, or by documenting results of periodic reviews. Example: 24-Dec-05
12	System Categorization		Select appropriate security categorization impact levels [Drop Down] Low Moderate High *Link to CNSSI 1253 for description* ***Information can be obtained from the Security Plan (Confidentiality/ Integrity/ Availability).***
13	Stakeholder Information		Identify the stakeholders who were consulted during this assessment (e.g., Information System Owner (ISO), Information System Security Manager (ISSM), other stakeholders as appropriate). Include the following type of information for each role: Name/Rank/Grade: Organization/Office: Email: Phone:
	Main Template		
14	Executive Summary		The RAR executive summary is developed as a coordinated effort between the PM/SM, and ISO using vulnerabilities identified by the SCA in the SAR. PM/SM in coordination with the ISO must determine and document in the RAR an assessment of overall system cybersecurity risk (Very Low, Low, Moderate, High, or Very High), and identify the key drivers for that assessment. PM/SM in coordination with the ISO provides an AO with a synopsis of the assessment report focusing on the security controls assessment to include overall description of security posture of the IS or PIT systems and an overall recommendation for authorization of the IS or PIT systems. Include recommendations for correcting or accepting risk due to specific vulnerabilities, as well as stipulating implementation of any of the proposed mitigations.
15	**Summary of Risk Assessment Results**	15a. Risk Determination	Use this table to plot the highest risk non-compliant security control (or enhancements) for each security objective (C-I-A). With regard to the aggregation of risk (multiple security controls plotting to similar risk), plot the security control with the highest risk to establish the upper bound for recording overall risk for each security objective. Indicate a C - I - A within the appropriate box as per the example. **Note:** When no non-compliant security control exist for a security objective, that security objective will not be mapped. When multiple security controls receive a risk rating of High or Very High, each is briefly discussed, as related to its assigned security objective, in the Executive Summary to the AO.
		15b. Non-Compliant Security Controls by Risk Level *(Before Mitigation)*	Identify the number of all non-compliant security controls (and enhancements) at each risk level, before any proposed mitigations are applied (i.e., what the risk is in the system's current state).

		15c. Non-Compliant Security Controls by Risk Level *(After Proposed Mitigation)*	Identify the number of all non-compliant security controls (and enhancements) at each risk level, after the proposed mitigations (i.e., what the risk would be if the PM implemented the listed proposed mitigations).
16		16a. Non-Compliant Security Controls	List the applicable security control/enhancement number associated with the vulnerability. If more than one security control is associated with a vulnerability, list all security controls on separate lines and repeat the vulnerability description.
		16b. Vulnerability Description (*From SAR)*	Describe the vulnerability associated with each non-compliant security control. ***Information can be obtained from the SAR (Vulnerability Summary).***
		16c. Security Objectives *(C-I-A)*	Identify the security objective (Confidentiality, Integrity, and/or Availability) supported by the security control/enhancement (reference CNSSI No. 1253, Table D-2, Additional Security Control Information) by using C, I, or A. In some cases security controls may support multiple security objectives and should be separated by a hyphen "-" (e.g., C-I or C-I-A or C-A or I-A).
		16d. Severity or Pervasiveness	The severity value is assigned to a vulnerability, but a pervasiveness value is assigned to predisposing conditions. The PM/SM estimates this value based on a comparison of the raw findings during the security controls assessment and the effectiveness of mitigation actions (see Table 3 on the RMF KS page "Model for Assessing Residual Risk Level for Non-Compliant Security Controls"). If mitigations are completely effective, this value is non-existent and the remainder of the cells in the row would contain no values, as there can be no likelihood of exploitation, impact, or risk. This value is informed by assessment at the control correlation identifier (CCI) level. If a control has a STIG or SRG associated through CCIs, the vulnerabilities identified by STIG or SRG assessments will be used to inform the value in this column for the security control, but there isn't a one-to-one correlation between raw STIG CAT values (i.e., CAT I, CAT II, CAT III) and this value. Identify the severity or pervasiveness as one of the following: Very Low (VL) Low (L) Moderate (M) High (H) Very High (VH)
		16e. Relevance of Threat	Determine the relevance of the threat by identifying potential threat events, relevance of the events, and threat sources that could initiate the events. If the relevance of the threat does not meet the organization's criteria for further consideration, do not complete the remaining columns, as there is no risk. This factor is based on the risk assessor's estimate after considering a combination of an adversarial threat source's capability, intent, and targeting or a non-adversarial threat source's range of effects based on available evidence, experience, and expert judgment. This factor takes into consideration multiple NIST SP 800-30 risk factors; that is, consider which threat sources may initiate which threat events against the vulnerability or predisposing condition. There is a many-to-many relationship between these risk factors. While this model simplifies this relationship and assignment of a value, it may be advantageous for risk assessors to review NIST SP 800-30 to understand the factors, examine the exemplar lists of these factors, and separately document how these relationships were examined and measured. (See Table 4 on the RMF KS page "Model for Assessing Residual Risk Level for Non-Compliant Security Controls" for descriptions of values assigned to threat relevance.) Identify the relevance of threat as one of the following: Very Low (VL) Low (L) Moderate (M) High (H) Very High (VH)
	Specific Vulnerability	16f. Likelihood (Cells 16d & 16e)	Determine the likelihood a threat event will be initiated or occur and result in adverse impacts (see Table 5 on the RMF KS page "Model for Assessing Residual Risk Level for Non-Compliant Security Controls" for likelihood values). Likelihood is a combination of likelihood of attack initiation/ occurrence and likelihood that initiated attack succeeds or the threat even results in adverse impact. If resource constraints allow, risk assessors may reference NIST SP 800-30 for guidance on determining this value (i.e., could use another 5x5 matrix to plot the two factors and determine the overall likelihood.) However, as the likelihood is summarized in this model, risk assessors assign a value by comparing the results of 16d. "Severity or Pervasiveness" with 16e. "Relevance of Threat." The factors from these two columns are plotted on a 5x5 matrix, and the intersection on the matrix indicates the value for likelihood (see tab "RAR Likelihood & Risk Matrices" for the 5x5 matrix). Identify the likelihood as one of the following: Very Low (VL) Low (L) Moderate (M) High (H) Very High (VH)
		16g. Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. Risk assessors may consider the Concept of Operations, system description, User Representative input, etc. (See Table 6 on the RMF KS page "Model for Assessing Residual Risk Level for Non-Compliant Security Controls" for descriptions of the values assigned to impact.) Identify the impact as one of the following: Very Low (VL) Low (L) Moderate (M) High (H) Very High (VH)
		16h. Impact Description	Describe the operational impact due to the non-compliant security control.
		16i. Risk (Cells 16f & 16g)	Determine the level of risk as a combination of likelihood and impact (see Table 7 on the RMF KS page "Model for Assessing Residual Risk Level for Non-Compliant Security Controls" for descriptions of values assigned to risk). Risk assessors assign a value by comparing the results of 16f. "Likelihood" with 16g. "Impact." The factors from these columns are plotted on a 5x5 matrix, and the intersection on the matrix indicates the value for risk (see tab "RAR Likelihood & Risk Matrices" for the 5x5 matrix). Identify the risk as one of the following: Very Low (VL) Low (L) Moderate (M) High (H) Very High (VH)
		16j. Proposed Mitigations	List the proposed mitigations that, if implemented, will reduce the risk.
		16k. Residual Risk *(After Initial Mitigation)*	Indicate the risk level expected after the initial mitigations are implemented. This mitigations are provided in the POA&M.
		16l. Recommendations	The PM/SM lists the recommendations addressing actions that will at a minimum reduce the High and Very High Risk non-compliant security controls to a Moderate Risk.

Combination of Vulnerability Severity/Predisposing Condition Pervasiveness and Threat Relevance

Relevance of Threat	Vulnerability Severity/Predisposing Condition Pervasiveness				
	Very Low	Low	Moderate	High	Very High
Very High	*Very Low*	*Low*	*Moderate*	*High*	*Very High*
High	*Very Low*	*Low*	*Moderate*	*High*	*Very High*
Moderate	*Very Low*	*Low*	*Moderate*	*Moderate*	*High*
Low	*Very Low*	*Low*	*Low*	*Low*	*Moderate*
Very Low	*Very Low*	*Very Low*	*Low*	*Low*	*Low*

Combination of Likelihood and Impact

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Impact				
	Very Low	Low	Moderate	High	Very High
Very High	*Very Low*	*Low*	*Moderate*	*High*	*Very High*
High	*Very Low*	*Low*	*Moderate*	*High*	*Very High*
Moderate	*Very Low*	*Low*	*Moderate*	*Moderate*	*High*
Low	*Very Low*	*Low*	*Low*	*Low*	*Moderate*
Very Low	*Very Low*	*Very Low*	*Low*	*Low*	*Low*

DoD Risk Assessment Report (RAR) of Non-Compliant Security Controls

(1) System Name	(2) System Acronym	(3) DoD Component	(4) System Identification	(5) System Type
<Insert System Name Here>				

(6) Authorizing Official	(8) Authorization Status	(9) Assessment Completion Date	(10) Period Covered		(11) Last Update
			Authorization Date	Authorization Termination Date	
(7) Security Controls Assessor (SCA) and/or SCA Representative		(12) System Categorization			(13) Stakeholder Information
		Confidentiality	Integrity	Availability	ISO:
					ISSM:
					Other:

(14) Executive Summary:

(15) Summary of Risk Assessment Results:

(15a) Risk Determination

Likelihood \ Impact	Very Low	Low	Moderate	High	Very High
Very High				7	12
High					
Moderate					
Low					
Very Low					

Legend
Very High
High
Moderate
Low
Very Low

(15b) Non-Compliant Security Controls by Risk Level *(Before Mitigation)*

Security Objectives \ Impact	Very Low	Low	Moderate	High	Very High
	5	3	6	4	2

(15c) Non-Compliant Security Controls by Risk Level *(After Proposed Mitigation)*

Security Objectives \ Impact	Very Low	Low	Moderate	High	Very High
	8	8	4	0	0