NIST AI RMF V1.0 PROFILE SCORECARD ©

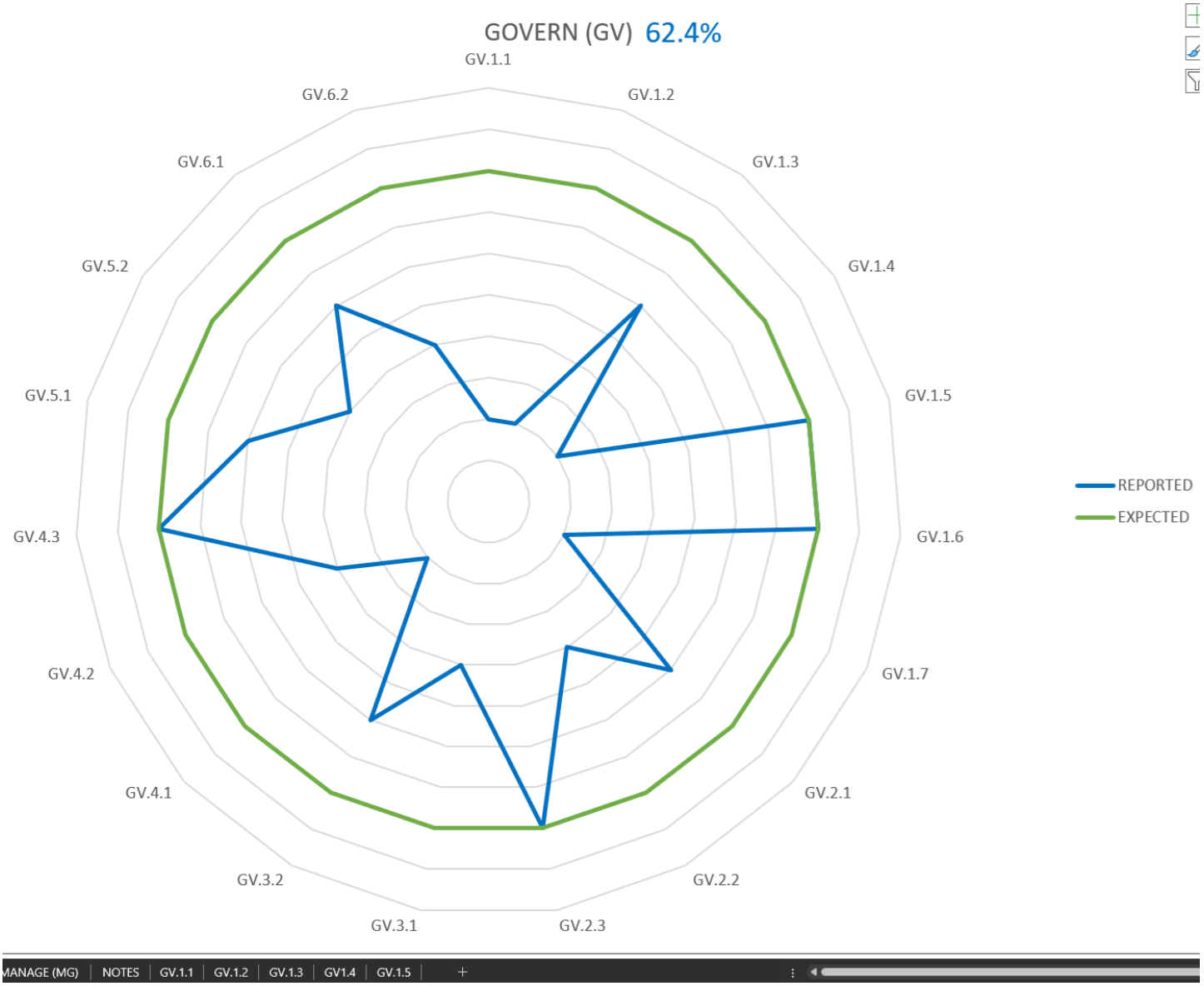
Govern GV	**62.4%**	*Protected Against Risk (Loss)*	$322,440,000
		Govern 1 *Effective Governance* GV.1	53.6%
		Govern 2 *Accountability Structures* GV.2	75.0%
		Govern 3 *Inclusive Workforce* GV.3	62.5%
		Govern 4 *Cultural Commitment* GV.4	58.3%
		Govern 5 *Engagement Processes* GV.5	62.5%
		Govern 6 *Policies and Procedures* GV.6	62.5%
Map MP	**67.3%**	*Protected Against Risk (Loss)*	$307,160,000
		Map 1 *Context Understanding* MP.1	70.8%
		Map 2 *System Categorization* MP.2	83.3%
		Map 3 *Capabilities Assessment* MP.3	70.0%
		Map 4 *Risk Mapping* MP.4	62.5%
		Map 5 *Impact Characterization* MP.5	50.0%
Measure MS	**64.1%**	*Protected Against Risk (Loss)*	$381,940,000
		Measure 1 *Metrics Application* MS.1	75.0%
		Measure 2 *Trustworthiness Evaluation* MS.2	73.1%
		Measure 3 *Risk Tracking* MS.3	58.3%
		Measure 4 *Feedback Assessment* MS.4	50.0%
Manage MG	**31.3%**	*Protected Against Risk (Loss)*	$233,620,000
		Manage 1 *Risk Management* MG.1	25.0%
		Manage 2 *Strategic Implementation* MG.2	25.0%
		Manage 3 *Third-Party Management* MG.3	25.0%
		Manage 4 *Risk Treatments* MG.4	50.0%

SWOPE NIST AI RMF V1.0 .XLSX GRC TOOL SNIPPETS

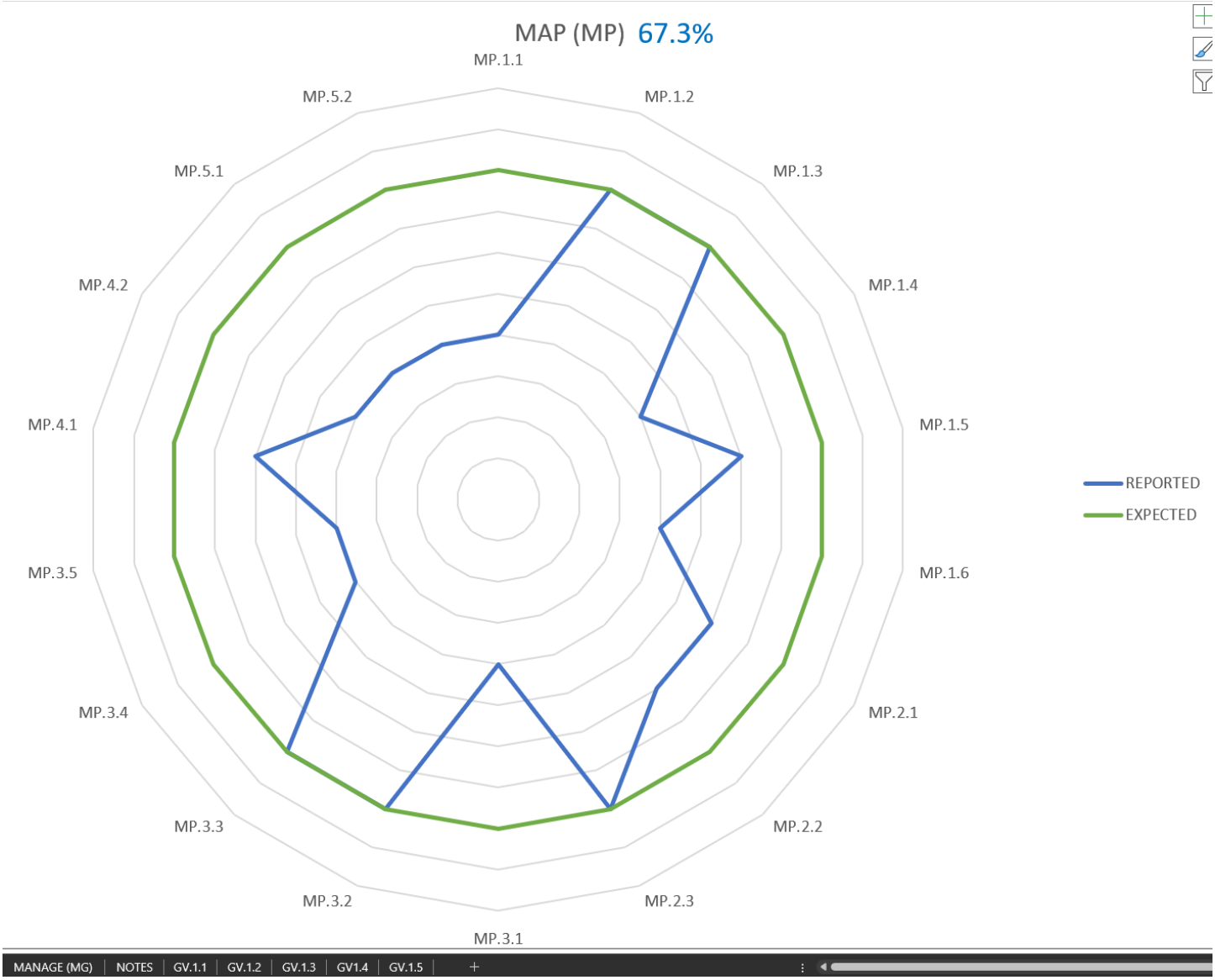
FUNCTION	STATE	EXP	%	CATEGORY	STATE	EXP	%	SUB-CATEGORY	
Govern GV	2.5	4.0	62.4%						
				Govern 1 Effective Governance GV.1	2.1	4.0	53.6%		
								GV.1.1	Legal and regulatory requirements involving AI are understood, ma
								GV.1.2	The characteristics of trustworthy AI are inte grated into organizat
								GV.1.3	Processes, procedures, and practices are in place to determine th
								GV.1.4	The risk management process and its outcomes are established t
								GV.1.5	Ongoing monitoring and periodic review of the risk management p
								GV.1.6	Mechanisms are in place to inventory AI systems and are resourc
								GV.1.7	Processes and procedures are in place for decommissioning and
				Govern 2 Accountability Structures GV.2	3.0	4.0	75.0%		
								GV.2.1	Roles and responsibilities and lines of communi cation related to
								GV.2.2	The organization?s personnel and partners receive AI risk manage
								GV.2.3	Executive leadership of the organization takes re sponsibility for d
				Govern 3 Inclusive Workforce GV.3	2.5	4.0	62.5%		
								GV.3.1	Decision-making related to mapping, measuring, and managing AI
								GV.3.2	Policies and procedures are in place to define and differentiate rol
				Govern 4 Cultural Commitment GV.4	2.3	4.0	58.3%		
								GV.4.1	Organizational policies and practices are in place to foster a critica
								GV.4.2	Organizational teams document the risks and po tential impacts o
								GV.4.3	Organizational practices are in place to enable AI testing, identifica
				Govern 5 Engagement Processes GV.5	2.5	4.0	62.5%		
								GV.5.1	Organizational policies and practices are in place to collect, consi
								GV.5.2	Mechanisms are established to enable the team that developed or
				Govern 6 Policies and Procedures GV.6	2.5	4.0	62.5%		
								GV.6.1	Policies and procedures are in place that address AI risks associa
								GV.6.2	Contingency processes are in place to handle failures or incidents
Map MP	2.7	4.0	67.3%						
				Map 1 Context Understanding MP.1	2.8	4.0	70.8%		
								MP.1.1	Intended purposes, potentially beneficial uses, context specific law
								MP.1.2	Interdisciplinary AI actors, competencies, skills, and capacities for
								MP.1.3	The organization?s mission and relevant goals for AI technology a
								MP.1.4	The business value or context of business use has been clearly de
								MP.1.5	Organizational risk tolerances are determined and documented.
								MP.1.6	System requirements (e.g., “the system shall respect the privacy o
				Map 2 System Categorization MP.2	3.3	4.0	83.3%		
								MP.2.1	The specific tasks and methods used to implement the tasks that
								MP.2.2	Information about the AI system?s knowledge limits and how syste
								MP.2.3	Scientific integrity and TEVV considerations are iden tified and doc
				Map 3 Capabilities Assessment MP.3	2.8	4.0	70.0%		
								MP.3.1	Potential benefits of intended AI system functionality and perform
								MP.3.2	Potential costs, including non-monetary costs, which result from e
								MP.3.3	Targeted application scope is specified and documented based or
								MP.3.4	Processes for operator and practitioner proficiency with AI systen
								MP.3.5	Processes for human oversight are defined, assessed, and docun
				Map 4 Risk Mapping MP.4	2.5	4.0	62.5%		
								MP.4.1	Approaches for mapping AI technology and legal risks of its comp
								MP.4.2	Internal risk controls for components of the AI system, including th
				Map 5 Impact Characterization MP.5	2.0	4.0	50.0%		
								MP.5.1	Likelihood and magnitude of each identified impact (both potential
								MP.5.2	Practices and personnel for supporting regular en gagement with r
Measure MS	2.6	4.0	64.1%						
				Measure 1 Metrics Application MS.1	3.0	4.0	75.0%		
								MS.1.1	Approaches and metrics for measurement of AI risks enumerated
								MS.1.2	Appropriateness of AI metrics and effectiveness of existing contr
								MS.1.3	Internal experts who did not serve as front-line developers for the s
				Measure 2 Trustworthiness Evaluation MS.2	2.9	4.0	73.1%		
								MS.2.1	Test sets, metrics, and details about the tools used during TEVV a
								MS.2.2	Evaluations involving human subjects meet ap plicable requiremer
								MS.2.3	AI system performance or assurance criteria are measured qualita
								MS.2.4	The functionality and behavior of the AI sys tem and its componer
								MS.2.5	The AI system to be deployed is demonstrated to be valid and relia
								MS.2.6	The AI system is evaluated regularly for safety risks – as identified
								MS.2.7	AI system security and resilience – as identified in the MAP functic
								MS.2.8	Risks associated with transparency and account ability – as identi
								MS.2.9	The AI model is explained, validated, and docu mented, and AI syst
								MS.2.10	Privacy risk of the AI system – as identified in the MAP function –
								MS.2.11	Fairness and bias – as identified in the MAP function – are evaluat
								MS.2.12	Environmental impact and sustainability of AI model training and m
								MS.2.13	Effectiveness of the employed TEVV met rics and processes in th
				Measure 3 Risk Tracking MS.3	2.3	4.0	58.3%		
								MS.3.1	Approaches, personnel, and documentation are in place to regular
								MS.3.2	Risk tracking approaches are considered for settings where AI risk
								MS.3.3	Feedback processes for end users and impacted communities to
				Measure 4 Feedback Assessment MS.4	2.0	4.0	50.0%		
								MS.4.1	Measurement approaches for identifying AI risks are connected to
								MS.4.2	Measurement results regarding AI system trustworthiness in deplo
								MS.4.3	Measurable performance improvements or declines based on cor
Manage MG	1.3	4.0	31.3%						
				Manage 1 Risk Management MG.1	1.0	4.0	25.0%		
								MG.1.1	A determination is made as to whether the AI system achieves its
								MG.1.2	Treatment of documented AI risks is prioritized based on impact, I
								MG.1.3	Responses to the AI risks deemed high priority, as identified by the
								MG.1.4	Negative residual risks (defined as the sum of all unmitigated risks
				Manage 2 Strategic Implementation MG.2	1.0	4.0	25.0%		
								MG.2.1	Resources required to manage AI risks are taken into account – a
								MG.2.2	Mechanisms are in place and applied to sustain the value of deplo
								MG.2.3	Procedures are followed to respond to and recover from a previou
								MG.2.4	Mechanisms are in place and applied, and respon sibilities are ass

SCORECARD | DATA | GOVERN (GV) | MAP (MP) | MEASURE (MS) | MANAGE (MG) | NOTES | GV.1.1 | GV.1.2

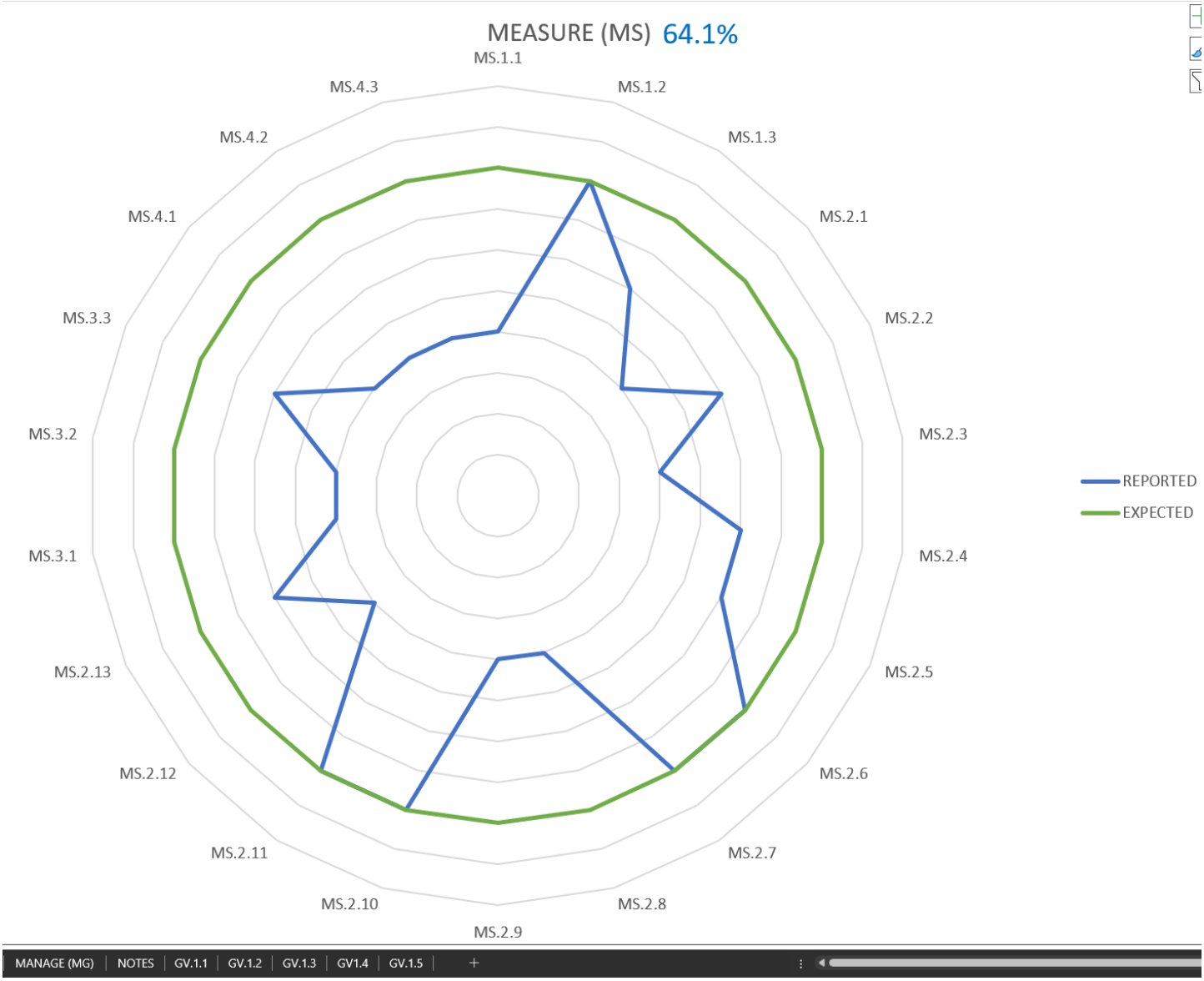
SWOPE NIST AI RMF V1.0 .XLSX GRC TOOL SNIPPETS

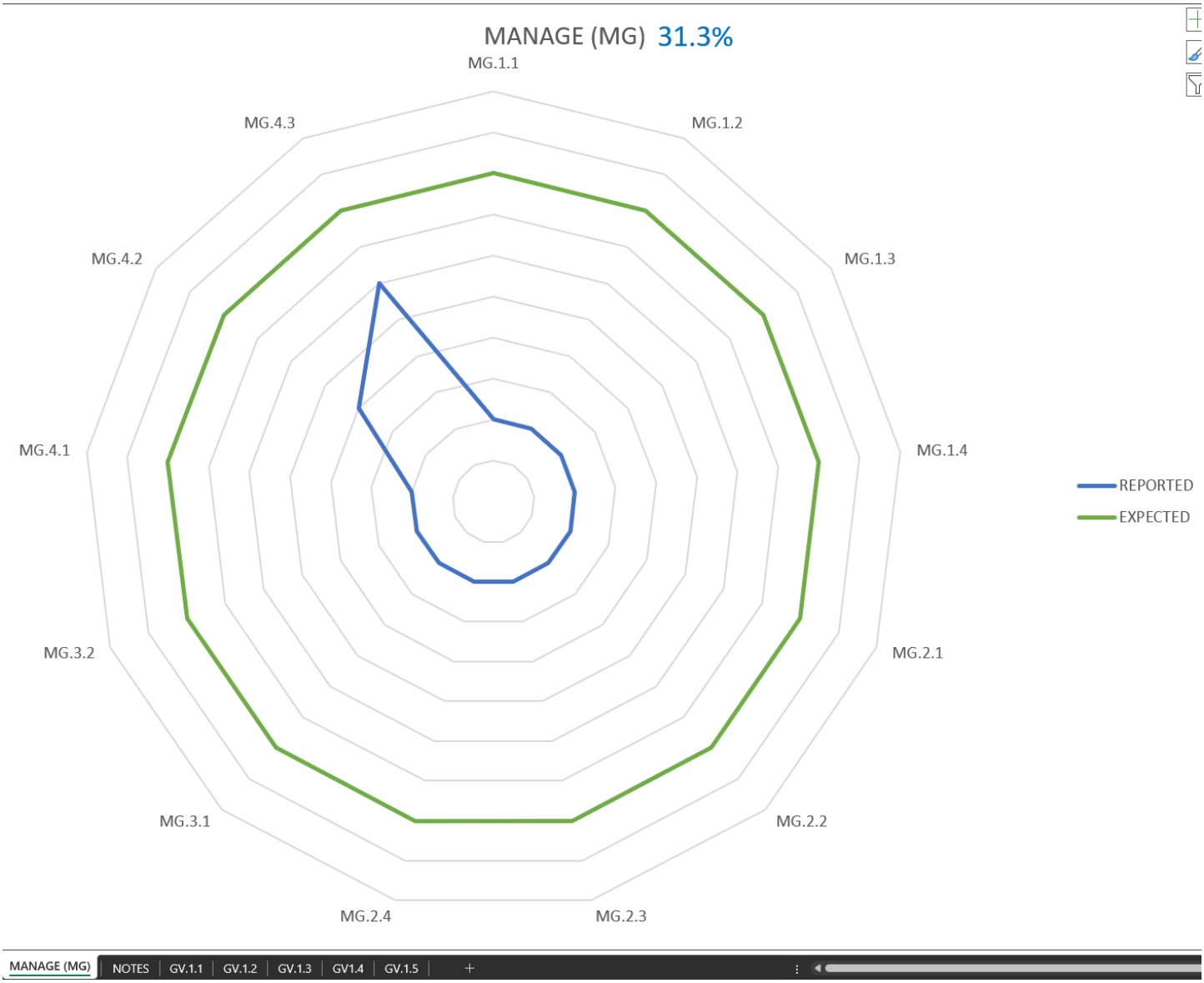


SWOPE NIST AI RMF V1.0 .XLSX GRC TOOL SNIPPETS



SWOPE NIST AI RMF V1.0 .XLSX GRC TOOL SNIPPETS




MANAGE (MG) 31.3%
MG.1.1
MG.1.2
MG.1.3
MG.1.4
MG.2.1
MG.2.2
MG.2.3
MG.2.4
MG.3.1
MG.3.2
MG.4.1
MG.4.2
MG.4.3
REPORTED
EXPECTED

SWOPE NIST AI RMF V1.0 .XLSX GRC TOOL SNIPPETS

NIST AI RMF V1.0 / 100-1	Artificial Intelligence Risk Management Framework (AI RMF 1.0)
4 Functional Areas	
19 Categories	
72 Subcategories	
360 Binary Responses	
3960 Survey Questions	
SCALE	Mapping Cyber Hygiene to the NIST Cybersecurity Framework (c
5.0 "World class, setting the standard"	
4.5 "Standard Operating Procedure, aligned with the business, aligned with best practices"	
4.0 "Standard Operating Procedure, Business as Usual (BAU)"	
3.5 "Occurs, consistently, aligned with ERM business risk and adversarial threat"	
3.0 "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"	
2.5 "Occurs, not consistently, structured"	
2.0 "Occurs, not consistently, unstructured"	
1.5 "Initial process and documentation in place"	
1.0 "ADHOC or only when necessary"	
0.5 "Awareness and acceptance of the need exists"	
0.0 "Not doing this at all"	
COST PROJECTIONS	
1 Labor Hour $ cost per each 72 Subcategories = 72 Labor Hours to fill out ATO Attestation Form/Questions	Authorization to Operate / Attestation of Security Assessment (
Knowledge Management/Intelligence = 28 Labor Hours to convert ATO data to KM Repo & Executive Dashboard	
TOTAL = 100 Labor Hours using Microsoft Suite (Excel, Sharepoint, PowerBI) x $72hr average FTE = **$7200 COST**	
*AI (GPT, LLMs) could increase efficiency (ex. ChatBots) & improve cost savings	
ADDITIONAL REFERENCE	
ISO	ISO/IEC 23894:2023 - Information technology — Artificial intellig
UC Berkeley	Berkeley-GPAIS-Foundation-Model-Risk-Management-Standard

SCORECARD | DATA | GOVERN (GV) | MAP (MP) | MEASURE (MS) | MANAGE (MG) | NOTES | GV.1.1 | GV.1.2 | GV.1.3 | GV1.4 | GV.1.5

SWOPE NIST AI RMF V1.0 .XLSX GRC TOOL SNIPPETS

GV.1.1	Legal and regulatory requirements involving AI are understood, managed, and documented.	Can you estimate the annualized frequency and potential financial impact of non-compliance events	[YES/NO]
	Level 5.0: "World class, setting the standard"		
		Does your organization set industry standards for AI legal and regulatory compliance?	[YES/NO]
		Is AI governance a core aspect of your organization's identity and values?	[YES/NO]
		Are AI legal and regulatory practices in your organization emulated by others?	[YES/NO]
		Does your organization contribute to developing legal frameworks for AI at a national or internationa	[YES/NO]
		Is your organization's approach to AI governance considered a benchmark for excellence?	[YES/NO]
	Level 4.5: "Standard Operating Procedure, aligned with the business, aligned with best practices"		
		Are AI legal requirements integrated into your organization's strategic planning?	[YES/NO]
		Does your organization benchmark its AI governance practices against industry best practices?	[YES/NO]
		Is there a continuous improvement process for AI legal and regulatory compliance?	[YES/NO]
		Are AI legal risks proactively managed and aligned with overall business goals?	[YES/NO]
		Is your organization recognized as a model for AI legal compliance in its sector?	[YES/NO]
	Level 4.0: "Standard Operating Procedure, Business as Usual (BAU)"		
		Is AI legal and regulatory compliance a standard part of every AI project?	[YES/NO]
		Are AI governance policies regularly reviewed and seamlessly integrated into business operations?	[YES/NO]
		Is training on AI legal issues mandatory and regular for all relevant personnel?	[YES/NO]
		Does your organization have a dedicated team for AI legal and regulatory compliance?	[YES/NO]
		Are documentation practices for AI compliance thorough and systematic?	[YES/NO]
	Level 3.5: "Occurs, consistently, aligned with ERM business risk and adversarial threat"		
		Is AI governance fully integrated into your organization's overall risk management?	[YES/NO]
		Are AI legal requirements consistently reviewed and aligned with business strategy?	[YES/NO]
		Does your organization proactively address AI legal risks in all projects?	[YES/NO]
		Is there an established, consistent training program on AI legal issues for all relevant staff?	[YES/NO]
		Are there robust processes for documenting and managing AI legal compliance?	[YES/NO]
	Level 3.0: "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"		
		Are AI legal requirements consistently integrated into project management?	[YES/NO]
		Is there a consistent process for updating AI governance policies?	[YES/NO]
		Does your organization regularly train staff on AI legal and regulatory issues?	[YES/NO]
		Are AI legal risks systematically identified and addressed in projects?	[YES/NO]
		Is there a clear, consistent approach to documenting AI compliance?	[YES/NO]
	Level 2.5: "Occurs, not consistently, structured"		
		Is there a structured but irregular process for reviewing AI's legal aspects?	[YES/NO]
		Are AI legal and regulatory requirements part of project planning, though not always?	[YES/NO]
		Does your organization periodically review and update its AI governance framework?	[YES/NO]
		Are there defined roles for managing AI legal risks, though not fully established?	[YES/NO]
		Is there a structured approach to training staff on AI legal issues, though not comprehensive?	[YES/NO]
	Level 2.0: "Occurs, not consistently, unstructured"		
		Are there instances where AI legal requirements are systematically reviewed?	[YES/NO]
		Is there an evolving understanding of AI's legal implications across the organization?	[YES/NO]
		Are legal discussions about AI becoming more frequent?	[YES/NO]
		Does your organization sporadically update AI governance policies?	[YES/NO]
		Are there informal but regular trainings or meetings about AI legal risks?	[YES/NO]
	Level 1.5: "Initial process and documentation in place"		
		Is there a preliminary policy for AI governance?	[YES/NO]
		Are legal and regulatory requirements for AI documented in any form?	[YES/NO]
		Does your organization have initial training for staff on AI legal issues?	[YES/NO]
		Are there initial efforts to standardize AI governance practices?	[YES/NO]
		Is there a basic checklist or framework for AI legal compliance?	[YES/NO]
	Level 1.0: "ADHOC or only when necessary"		
		Are legal and regulatory aspects considered in AI project planning?	[YES/NO]
		Is there a basic framework for AI governance, though used inconsistently?	[YES/NO]
		Are AI legal requirements discussed in specific project meetings?	[YES/NO]
		Does your organization consult legal experts for AI-related projects when necessary?	[YES/NO]
		Are there ad-hoc procedures for documenting AI compliance issues?	[YES/NO]
	Level 0.5: "Awareness and acceptance of the need exists"		
		Is there a designated team or individual responsible for AI governance?	[YES/NO]
		Has your organization identified specific legal standards applicable to AI?	[YES/NO]
		Are there informal discussions about AI's legal and regulatory risks?	[YES/NO]
		Is there awareness of the need for AI risk management?	[YES/NO]
		Has the need for documenting AI-related legal issues been recognized?	[YES/NO]
	Level 0.0: "Not doing this at all"		
		Is there any acknowledgement of AI in your organization's legal or regulatory discussions?	[YES/NO]
		Has your organization identified any legal or regulatory requirements related to AI?	[YES/NO]
		Does your organization recognize the potential legal implications of using AI?	[YES/NO]
		Is there an understanding of the importance of AI governance?	[YES/NO]
		Are AI systems considered in any compliance discussions?	[YES/NO]

SCORECARD | DATA | GOVERN (GV) | MAP (MP) | MEASURE (MS) | MANAGE (MG) | NOTES | GV.1.1 | GV.1.2 | GV.1.3 | GV1.4 | GV.1.5 | +

SWOPE NIST AI RMF V1.0 .XLSX GRC TOOL SNIPPETS

GV.1.2	The characteristics of trustworthy AI are integrated into organizational policies, processes, proc	Can you estimate the potential annual financial impact, including costs associated with non-compliance, operatior	[YES/NO]
	Level 5.0: "World class, setting the standard"		
		Does your organization set industry standards for ethical AI governance and compliance?	[YES/NO]
		Is ethical AI governance a core aspect of your organization's identity and values?	[YES/NO]
		Are your organization's ethical AI practices emulated by others in the industry?	[YES/NO]
		Does your organization contribute to developing ethical frameworks for AI at a national or international level?	[YES/NO]
		Is your organization's approach to ethical AI governance considered a benchmark for excellence?	[YES/NO]
	Level 4.5: "Standard Operating Procedure, aligned with the business, aligned with best practices"		
		Are ethical AI considerations integrated into your organization's strategic planning?	[YES/NO]
		Does your organization benchmark its ethical AI practices against industry best practices?	[YES/NO]
		Is there a continuous improvement process for ethical AI governance?	[YES/NO]
		Are ethical AI risks proactively managed and aligned with overall business goals?	[YES/NO]
		Is your organization recognized as a model for ethical AI practices in its sector?	[YES/NO]
	Level 4.0: "Standard Operating Procedure, Business as Usual (BAU)"		
		Is ethical AI compliance a standard part of every AI project in your organization?	[YES/NO]
		Are ethical AI policies regularly reviewed and integrated into business operations?	[YES/NO]
		Is training on ethical AI issues mandatory and regular for all relevant personnel?	[YES/NO]
		Does your organization have a dedicated team for ethical AI compliance and governance?	[YES/NO]
		Are documentation practices for AI's ethical compliance thorough and systematic?	[YES/NO]
	Level 3.5: "Occurs, consistently, aligned with ERM business risk and adversarial threat"		
		Is ethical AI governance fully integrated into your organization's overall risk management?	[YES/NO]
		Are AI systems' ethical considerations consistently reviewed and aligned with business strategy?	[YES/NO]
		Does your organization proactively manage ethical risks in all AI projects?	[YES/NO]
		Is there a consistent training program on ethical AI for all relevant staff?	[YES/NO]
		Are robust processes for documenting and managing AI ethical compliance in place?	[YES/NO]
	Level 3.0: "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"		
		Are ethical considerations consistently integrated into AI project management?	[YES/NO]
		Does your organization have a consistent process for updating ethical AI policies?	[YES/NO]
		Are staff regularly trained on ethical AI issues and the organization's related policies?	[YES/NO]
		Are AI ethical risks systematically identified and addressed in projects?	[YES/NO]
		Is there a clear, consistent approach to documenting AI systems' adherence to ethical standards?	[YES/NO]
	Level 2.5: "Occurs, not consistently, structured"		
		Is there a structured process for ethical review of AI projects, though not consistently applied?	[YES/NO]
		Are AI systems' alignment with ethical standards part of the project planning process?	[YES/NO]
		Does your organization periodically review and update its ethical AI policies?	[YES/NO]
		Are roles for managing AI ethics starting to be defined within the organization?	[YES/NO]
		Is there a structured approach to training staff on ethical AI issues?	[YES/NO]
	Level 2.0: "Occurs, not consistently, unstructured"		
		Are there instances where AI systems are reviewed for ethical implications?	[YES/NO]
		Does your organization periodically update its understanding of trustworthy AI?	[YES/NO]
		Are ethical AI discussions becoming more frequent and relevant in project planning?	[YES/NO]
		Is there sporadic but noticeable effort in documenting AI systems' alignment with ethical standards?	[YES/NO]
		Does your organization have informal but regular meetings to discuss AI ethics?	[YES/NO]
	Level 1.5: "Initial process and documentation in place"		
		Has your organization begun to document policies related to trustworthy AI?	[YES/NO]
		Are there initial training programs on ethical AI for staff involved in AI projects?	[YES/NO]
		Is there a rudimentary policy framework for integrating trustworthy AI characteristics?	[YES/NO]
		Does your organization have a basic risk assessment process for AI systems?	[YES/NO]
		Are initial efforts being made to align AI systems with organizational values?	[YES/NO]
	Level 1.0: "ADHOC or only when necessary"		
		Are trustworthy AI characteristics considered in specific AI projects on an ad-hoc basis?	[YES/NO]
		Does your organization have any preliminary guidelines for ethical AI use?	[YES/NO]
		Are AI ethical considerations included in some project discussions or reviews?	[YES/NO]
		Is there an ad-hoc approach to addressing AI transparency and accountability?	[YES/NO]
		Does your organization consult external experts for ethical AI guidance when necessary?	[YES/NO]
	Level 0.5: "Awareness and acceptance of the need exists"		
		Has your organization identified key stakeholders for implementing trustworthy AI policies?	[YES/NO]
		Is there a basic understanding of what constitutes trustworthy AI in your organization?	[YES/NO]
		Are there informal discussions about the ethical implications of AI within your organization?	[YES/NO]
		Has your organization started to consider how AI systems align with its values and principles?	[YES/NO]
		Is there a recognition of the need for policies to govern AI systems?	[YES/NO]
	Level 0.0: "Not doing this at all"		
		Does your organization currently consider the integration of trustworthy AI characteristics in any of its policies or pr	[YES/NO]
		Is there any awareness in your organization about the importance of trustworthy AI?	[YES/NO]
		Has your organization recognized the need to align AI systems with ethical principles?	[YES/NO]
		Are there discussions about the potential risks associated with AI systems?	[YES/NO]
		Does your organization acknowledge the importance of transparency in AI systems?	[YES/NO]