

An Infinite Game: Cybersecurity Governance and Risk Management

By: Dan Holland

April 17, 2024

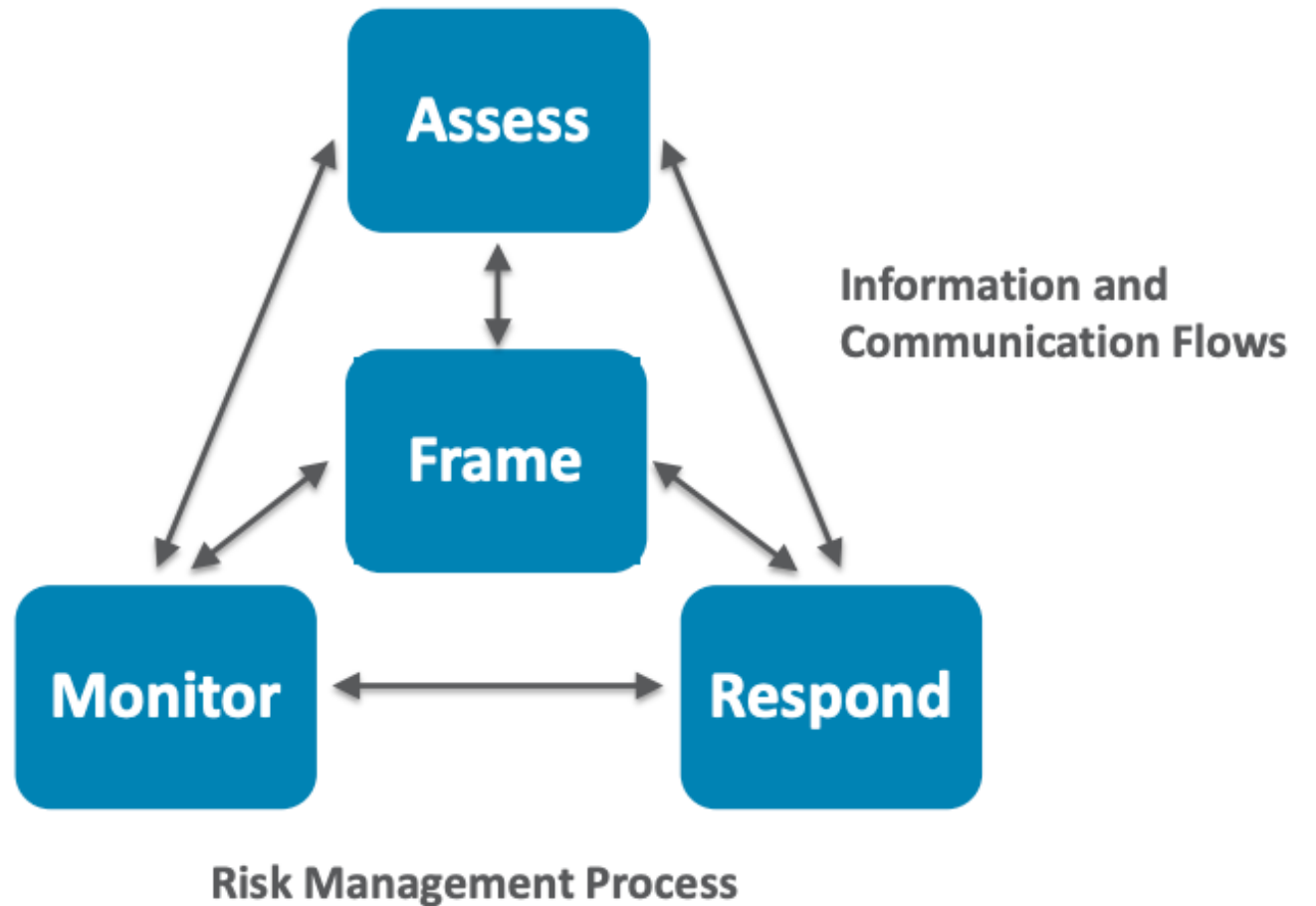


This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Arete Solutions.

Complexity is the enemy of security.



Four Risk Management Processes

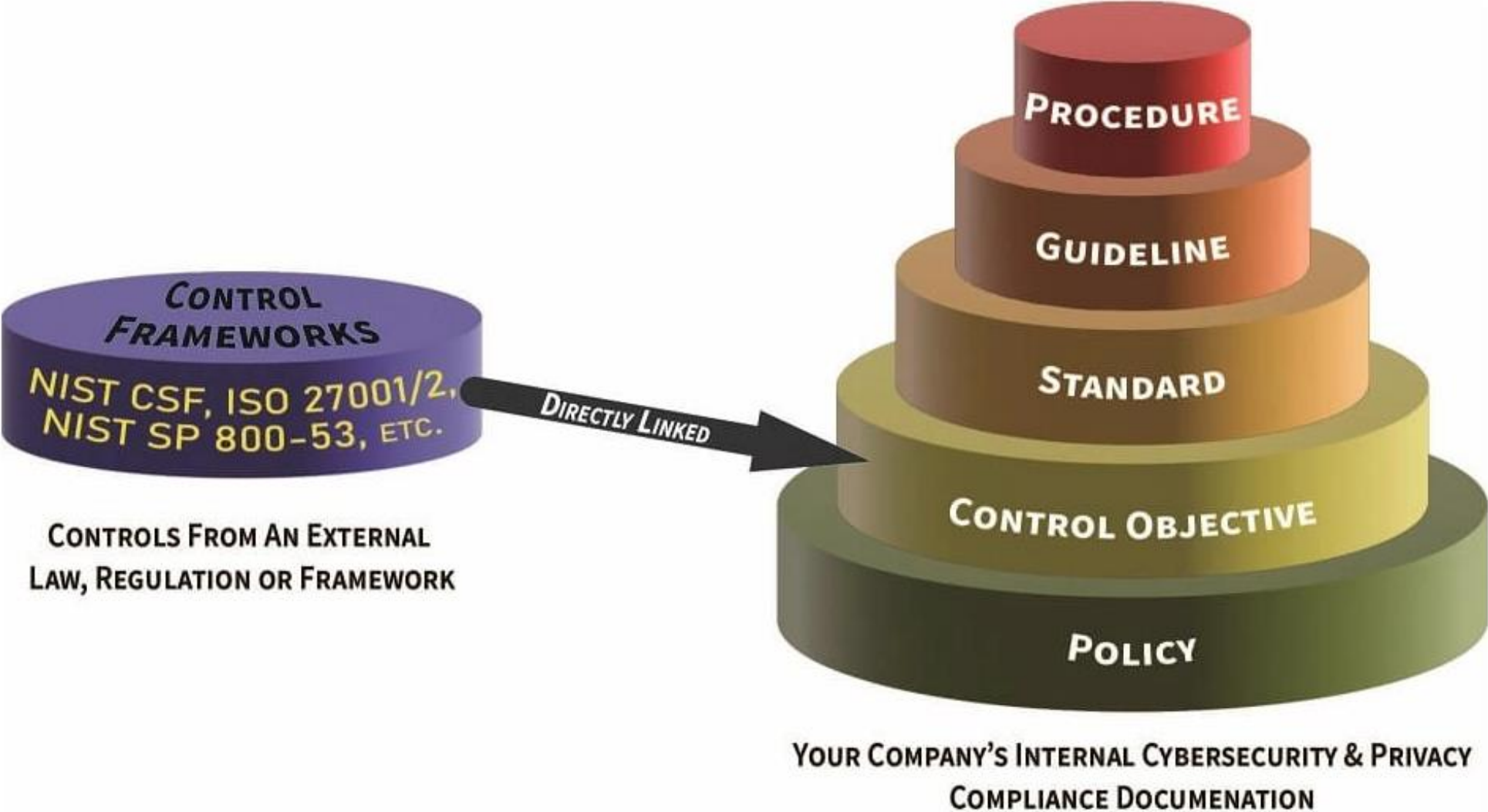


Process #1: Risk Framing

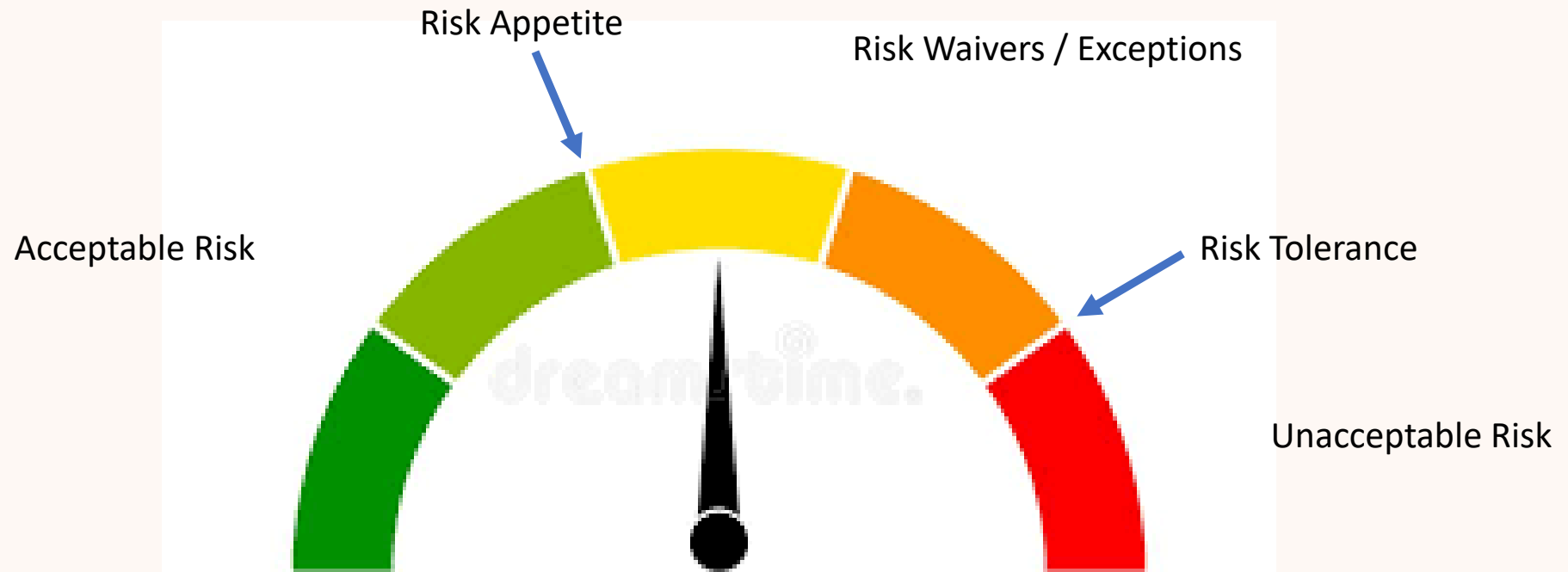
Produces a *Risk Management Policy* that establishes the foundation for risk-based decision making.



Hierarchy of Documentation

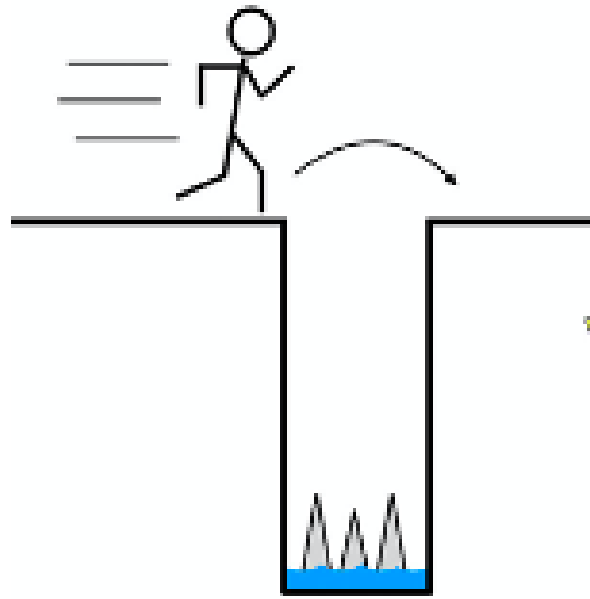


Risk Appetite & Risk Tolerance

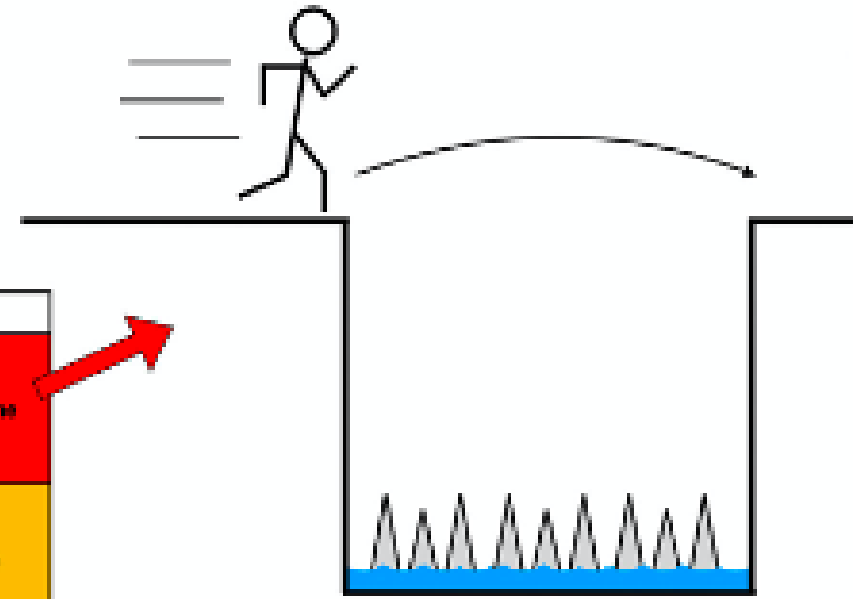


Process #2: Assessment



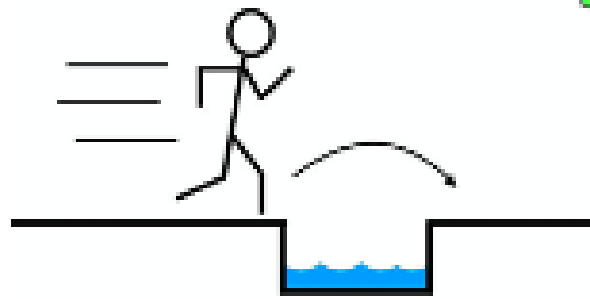


Low Probability & High Impact

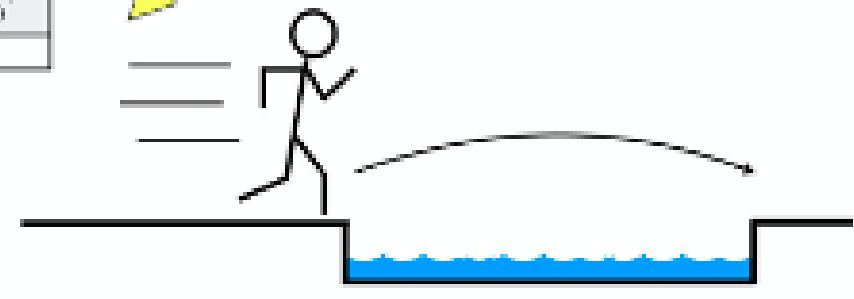


High Probability & High Impact

Risk Assessment Matrix				
Impact of Risk (Consequence)	Major Impact	Medium	High	Extreme
	Moderate Impact	Medium	Medium	High
	Minor Impact	Low	Medium	Medium
Risk Exposure = Impact x Probability		Unlikely (2-3%)	Moderate Likely (20%-60%)	Very Likely (60%+)
Probability of Risk (Likelihood)				



Low Probability & Low Impact



High Probability & Low Impact

Trying to explain our current
cyber risk to the board



**KEY PROBLEM:
THIS TYPE OF RISK
REPORTING
DOESN'T RESULT IN
BETTER DECISION-
MAKING.**

Impact

Severe (5)	1	2	5	8	2
Major (4)	1	2	8	7	8
Moderate (3)		6	16	9	4
Minor (2)		3	6		1
Insignificant (1)					
	Remote (1)	Rare (2)	Possible (3)	Probable (4)	Expected (5)

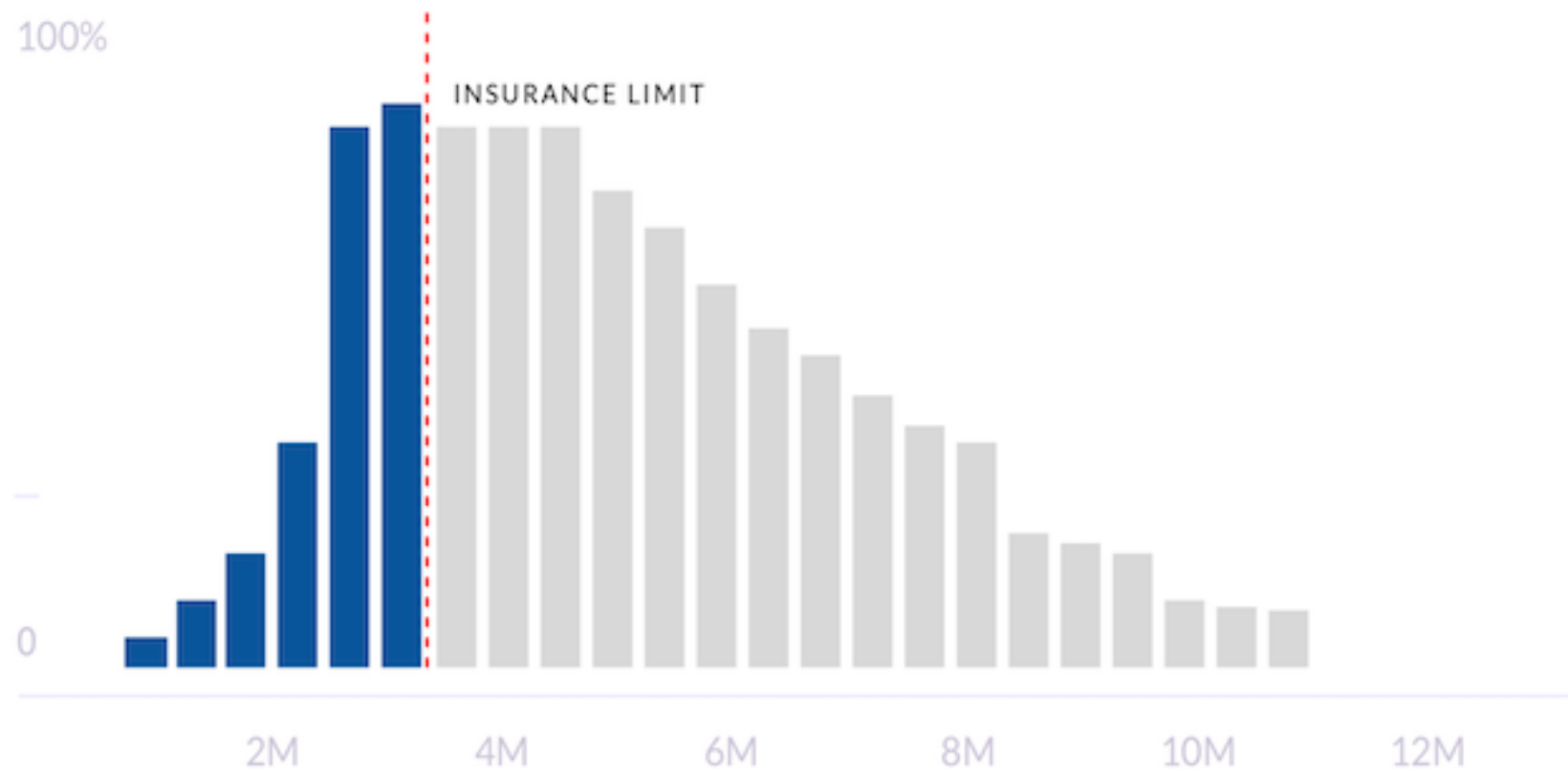
Probability

Ransomware - IT Servers and Endpoints ✓

SCENARIO DESCRIPTION

Ransomware destroys data on 50% of the organization's enterprise IT servers and endpoints (desktop and laptop computers). Affected endpoints and servers are functionally bricked, and require full replacement.

LOSS EXCEEDANCE CURVE



RISK SUMMARY

Calculation of Lost

\$2M
EXPECTED

\$1M_{MIN}
\$4M_{MAX}

Qualified of Impacts

5

Impacts with Relevant Coverage

2

INSURANCE SUMMARY

Total Coverage

\$1.8M

Policy B Coverage

\$700k

👍 0 👎 1

Policy C Coverage

\$100k

👍 0 👎 1

Policy A Coverage

\$1M

👍 0 👎 1

\$200k UNCOVERED

Process #3: Respond



Don't put a
\$10 fence
around a
\$5 horse.



Sample #1: CSF Target Profile Heat Map

Individual Score (1-4) Heat Map

Evaluating by functional area provides greater insight

Comparing Scores

Significant differences can highlight visibility issues and focus areas

IDENTIFY	SME INDIVIDUAL FUNCTIONAL AREA SCORES						SCORES		RESULTS		
	POLICY	NETWORK	ENDPOINT/ DATA PROTECTION	IDENTITY	OPs	APPs	SME AVERAGE	CORE GROUP	COMBINED SCORE SME AND CORE	TIER TARGET SCORE	RISK GAP
Business Environment	3	3	3	2	3	2	3	2	2	3	1
Asset Management	3	2	2	2	1	3	2	3	3	3	0
Governance	3	2	3	2	2	2	2	2	2	2	0
Risk Assessment	2	2	2	2	2	3	2	1	2	3	1
Risk Management Strategy	4	3	2	2	2	2	3	2	2	4	2
PROTECT											
Access Control	2	3	2	2	3	2	3	2	2	3	1
Awareness/Training	2	3	3	2	3	3	3	3	3	4	1
Data Security	2					2	2	3	3	3	0
Protective Process/Procedures Maintenance	2					2	2	2	2	4	2
Maintenance	3	2	2	2	2	4	2	1	2	3	1
Protective Technologies	2	2	1	3	1	2	2	3	2	3	1
DETECT											
Anomalies/Events	2	3	1	2	2	4	2	2	2	4	2
Security Continuous Monitoring	2	2	1	2	1	1	1	2	2	4	2
Detection Process	2	3	2	2	3	2	2	4	3	3	0
Threat Intelligence	3	3	3	2	2	2	3	3	3	3	0
RESPOND											
Response Planning	2	2	3	2	3	2	2	2	2	4	2
Communication	2	2	3	2	2	3	3	1	2	3	1
Analysis	2	3	3	2	3	3	3	2	2	3	1
Mitigations	2	3	1	2	3	1	2	3	3	3	0
Improvements	3	3	3	3	3	3	2	1	2	2	0
RECOVER											
Recovery Planning	2	3	3	2	2	2	3	3	3	3	0
Improvements	1	3	2	1	1	1	2	1	2	2	0
Communications	2	2	3	2	2	2	2	3	3	3	0

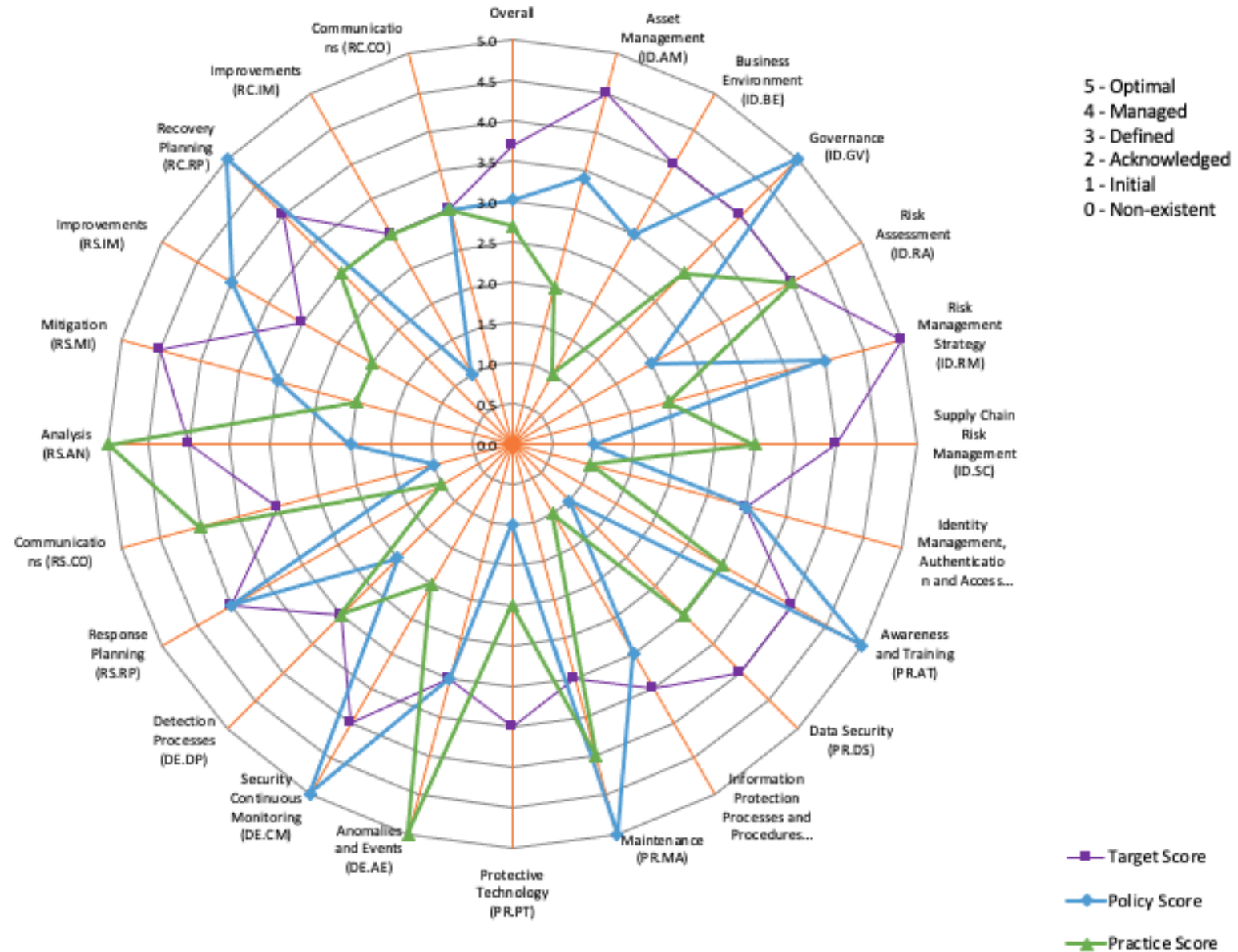
Mapping highlighted outliers and major differences

Significant differences between Core and Individual scores can highlight visibility issues

Focus areas stand out (large Δ)

NIST Cyber Security Framework Maturity Levels

Sample #2: CSF Target Profile Spider Chart



Process #4: Monitor

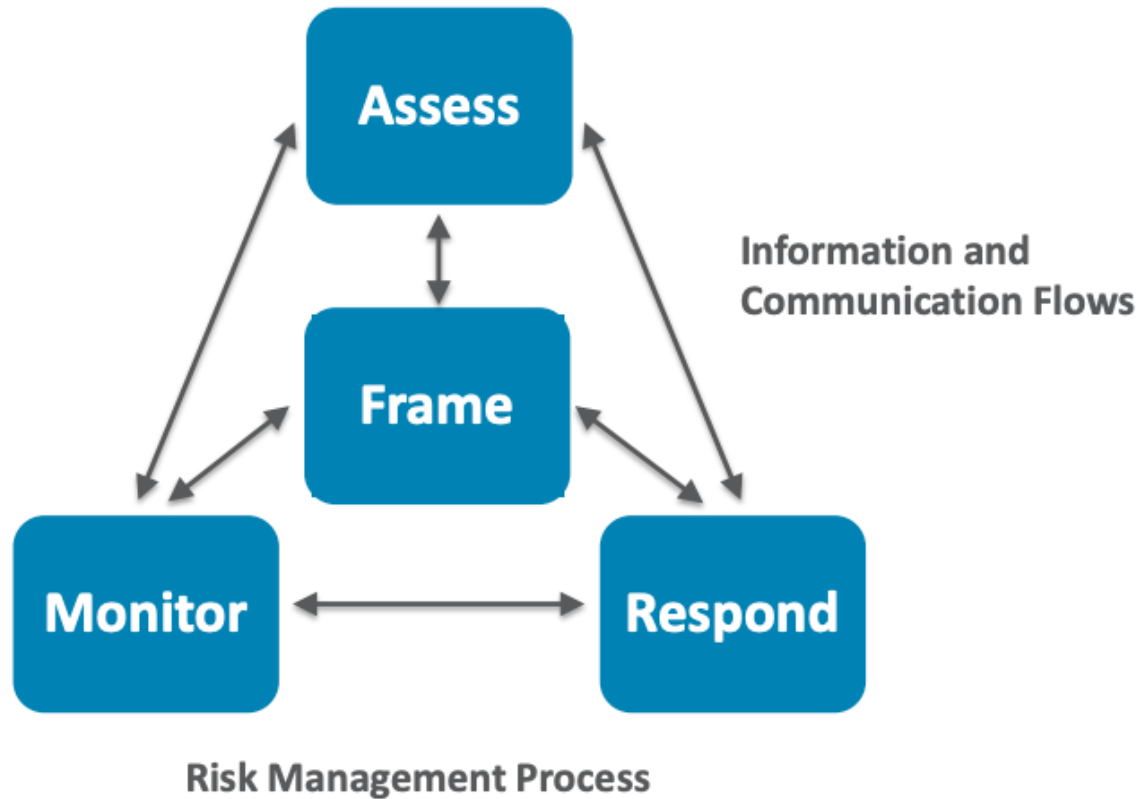


Notional Cybersecurity Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1											
2											
3											
4											
5											

Continually Communicate, Learn and Update

Recap: Infinite Game



Key NIST References

NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF)

NIST SP 800-39, Managing Information Security Risk

NIST SP 800-37, Risk Management Framework

FIPS 199, Standards for Security Categorization of Information Systems

FIPS 200, Minimum Security Requirements for Information Systems

NIST SP 800-53, Security and Privacy Controls for Information Systems

NIST SP 800-53A, Assessing Security and Privacy Controls in Information Systems

NIST SP 800-53B, Control Baselines for Information Systems

NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices

NIST SP 800-30, Guide for Conducting Risk Assessments

NIST IR 8286, Integrating Cybersecurity and Enterprise Risk Management



ARÊTE
SOLUTIONS



**CYBER
FLORIDA**

CONTINUE THE CONVERSATION

Dan Holland, Cybersecurity Risk Advisor

- Coast Guard Veteran
- 17 years experience

Dan.Holland@aretolutions.com

DTHolland@cyberflorida.org

