An Infinite Game: Cybersecurity Governance and Risk Management

By: Dan Holland

April 17, 2024

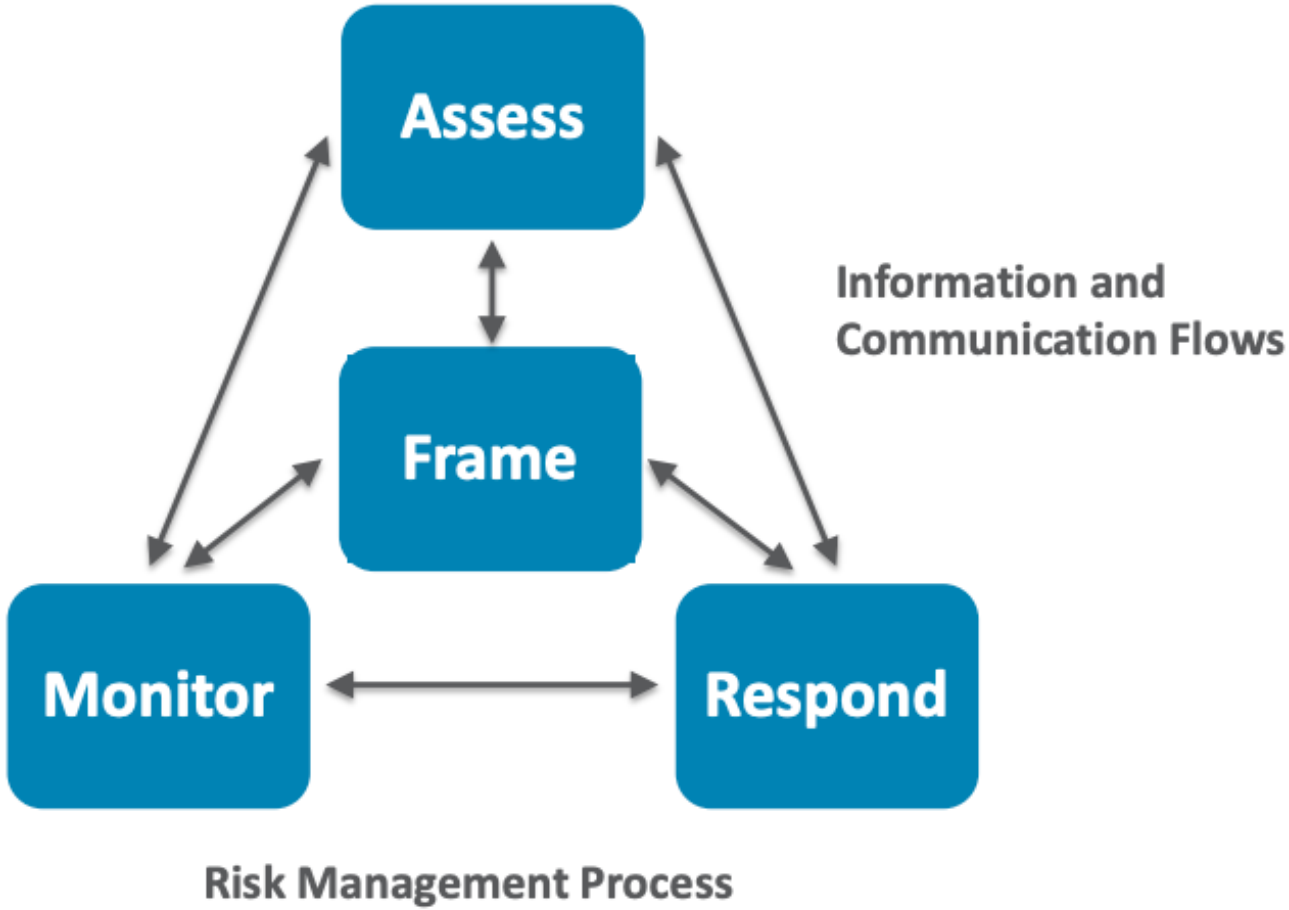
ARÊTE SOLUTIONS

CYBER FLORIDA

Complexity is the enemy of security.

Source: Sounil Yu

Four Risk Management Processes

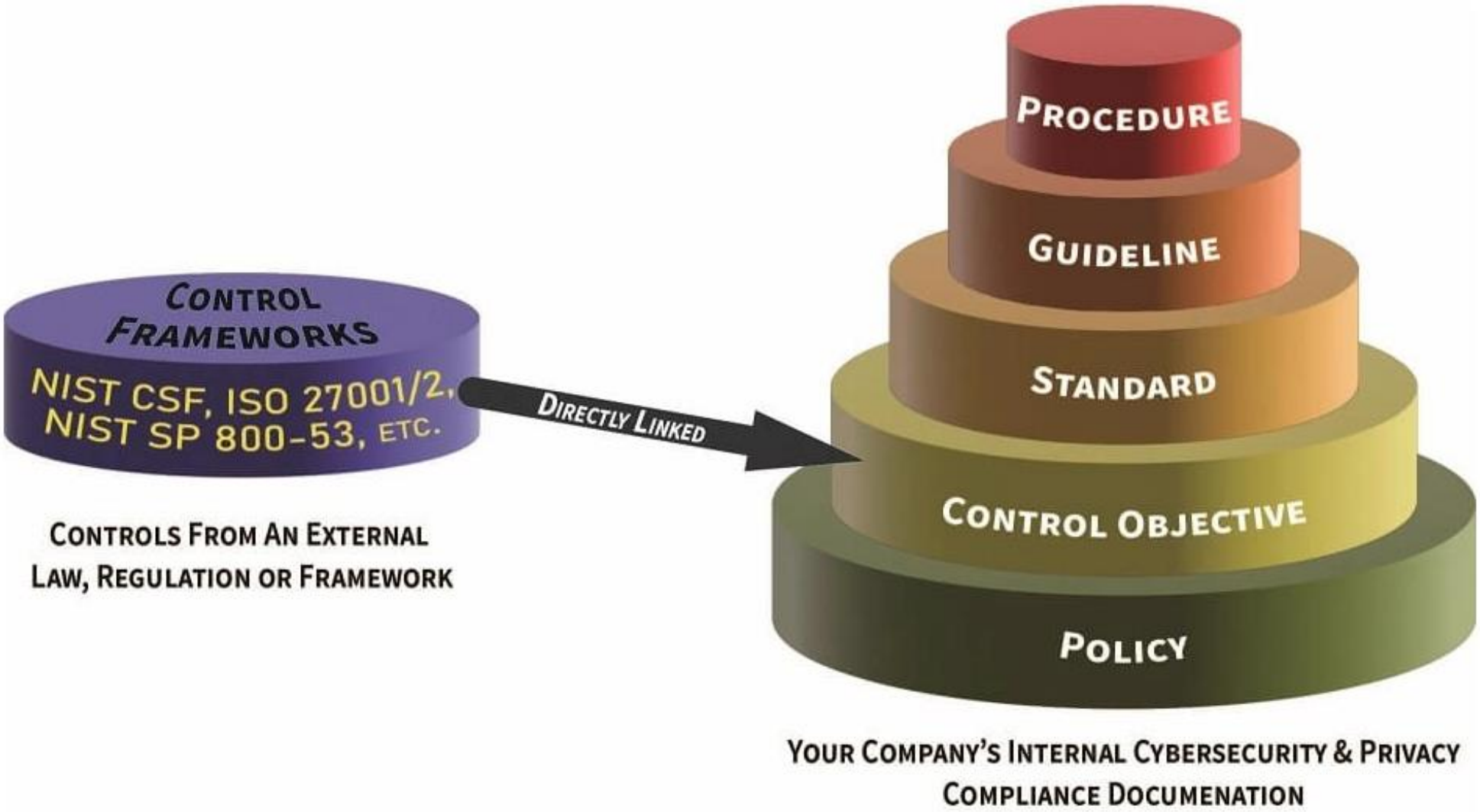


Source: NIST SP 800-39

Process #1: Risk Framing

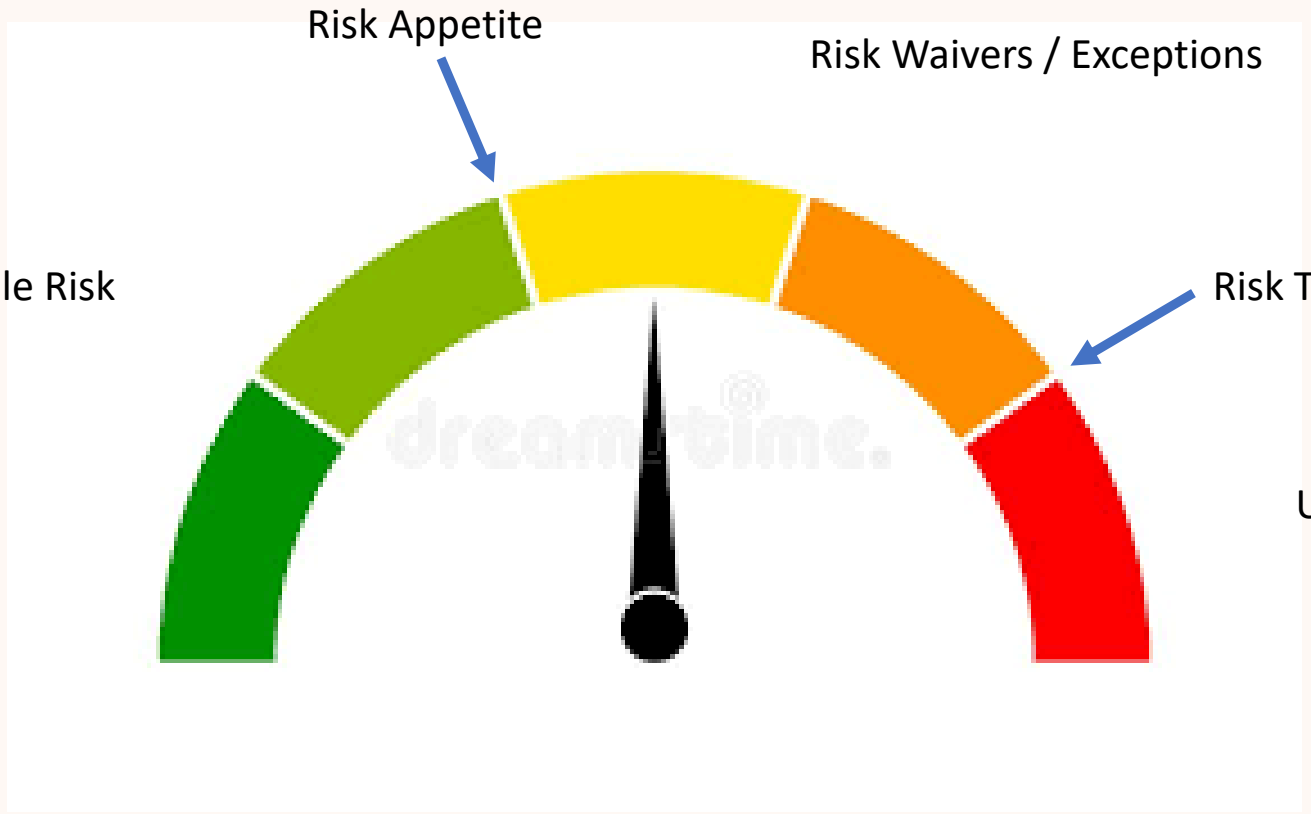
Produces a *Risk Management Policy* that establishes the foundation for risk-based decision making.

Hierarchy of Documentation



Ref: Compliance Forge

Risk Appetite & Risk Tolerance



ARÊTE
SOLUTIONS

Process #2: Assessment

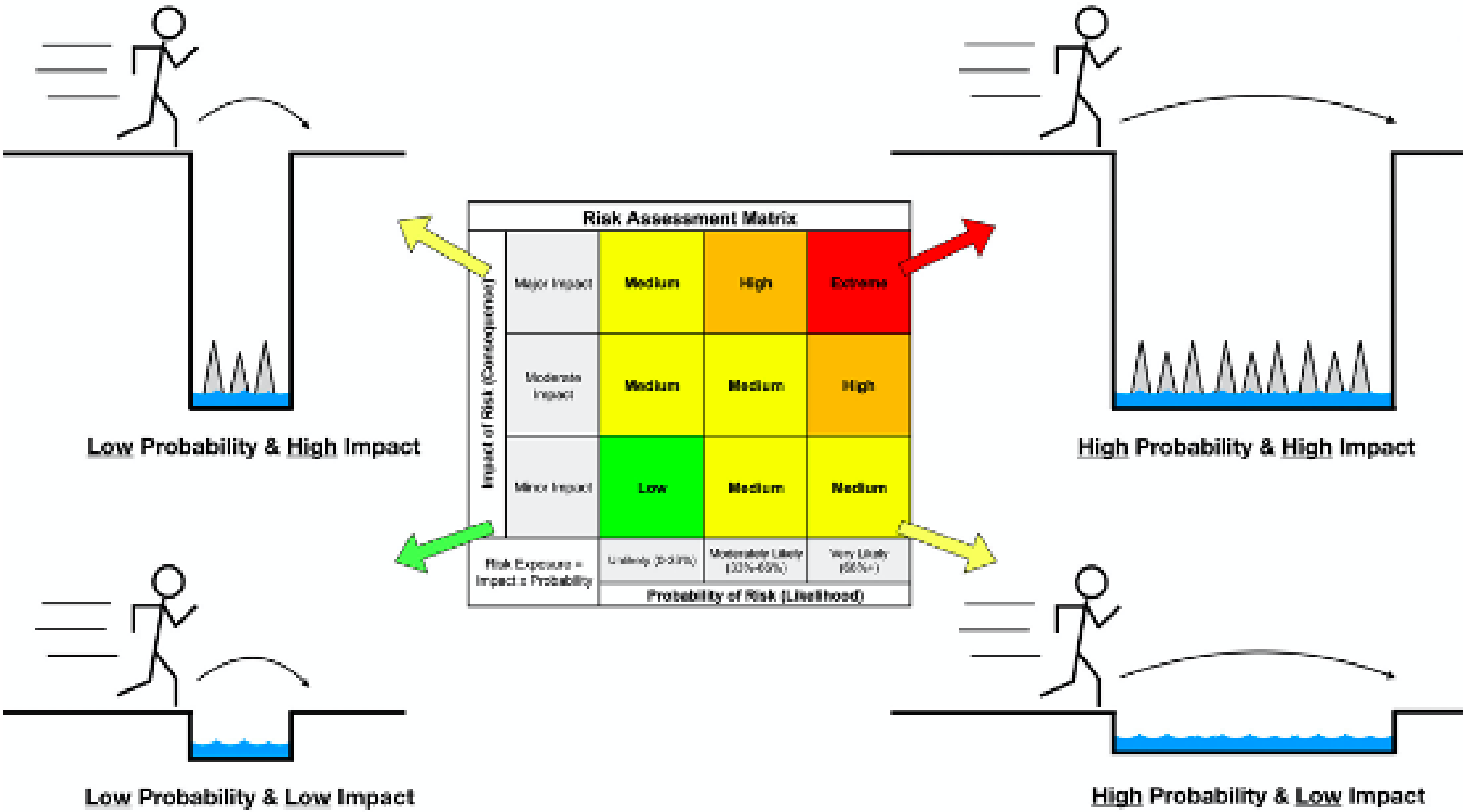
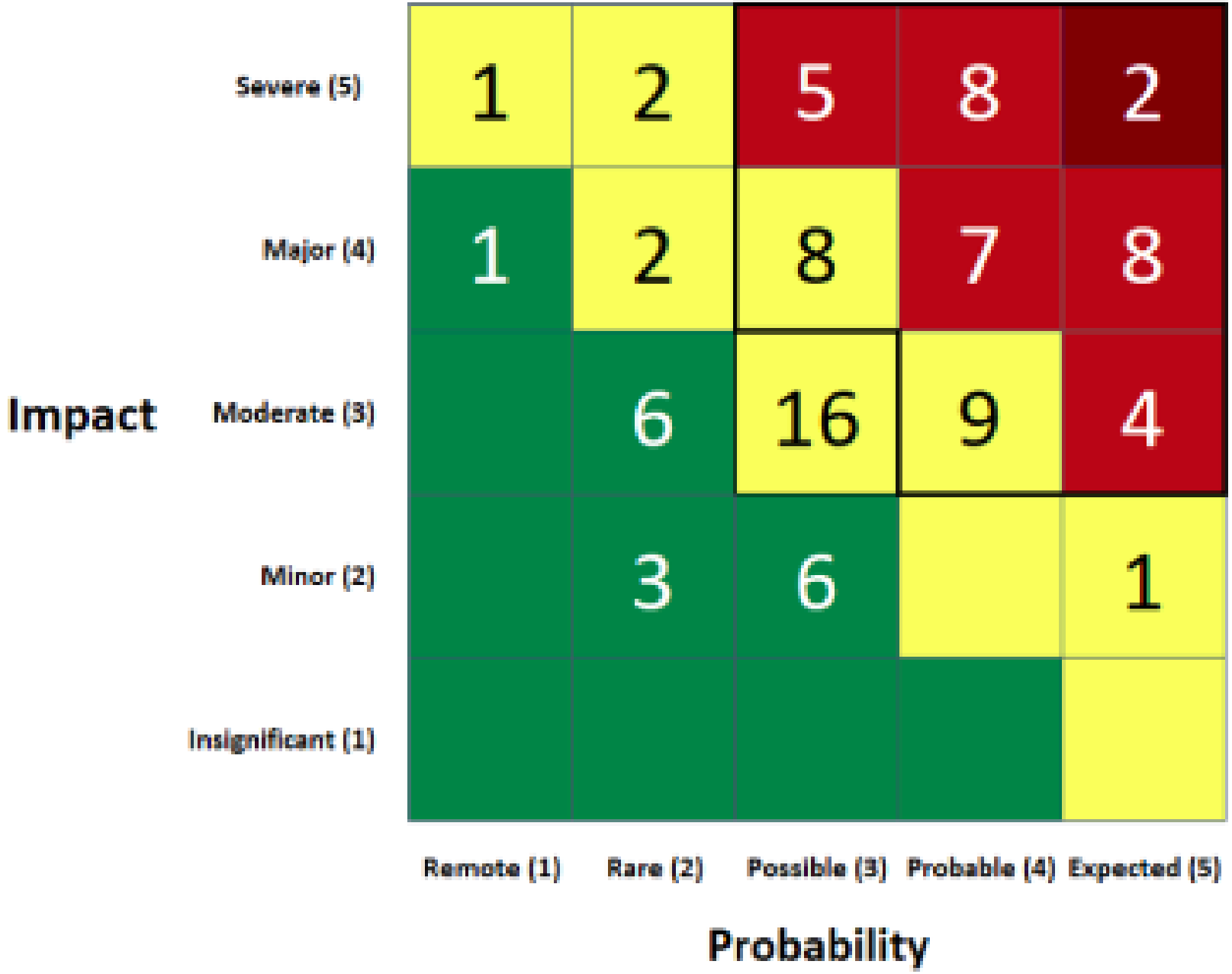


Image credit: theprojectmanagementblueprint.com

Trying to explain our current cyber risk to the board

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

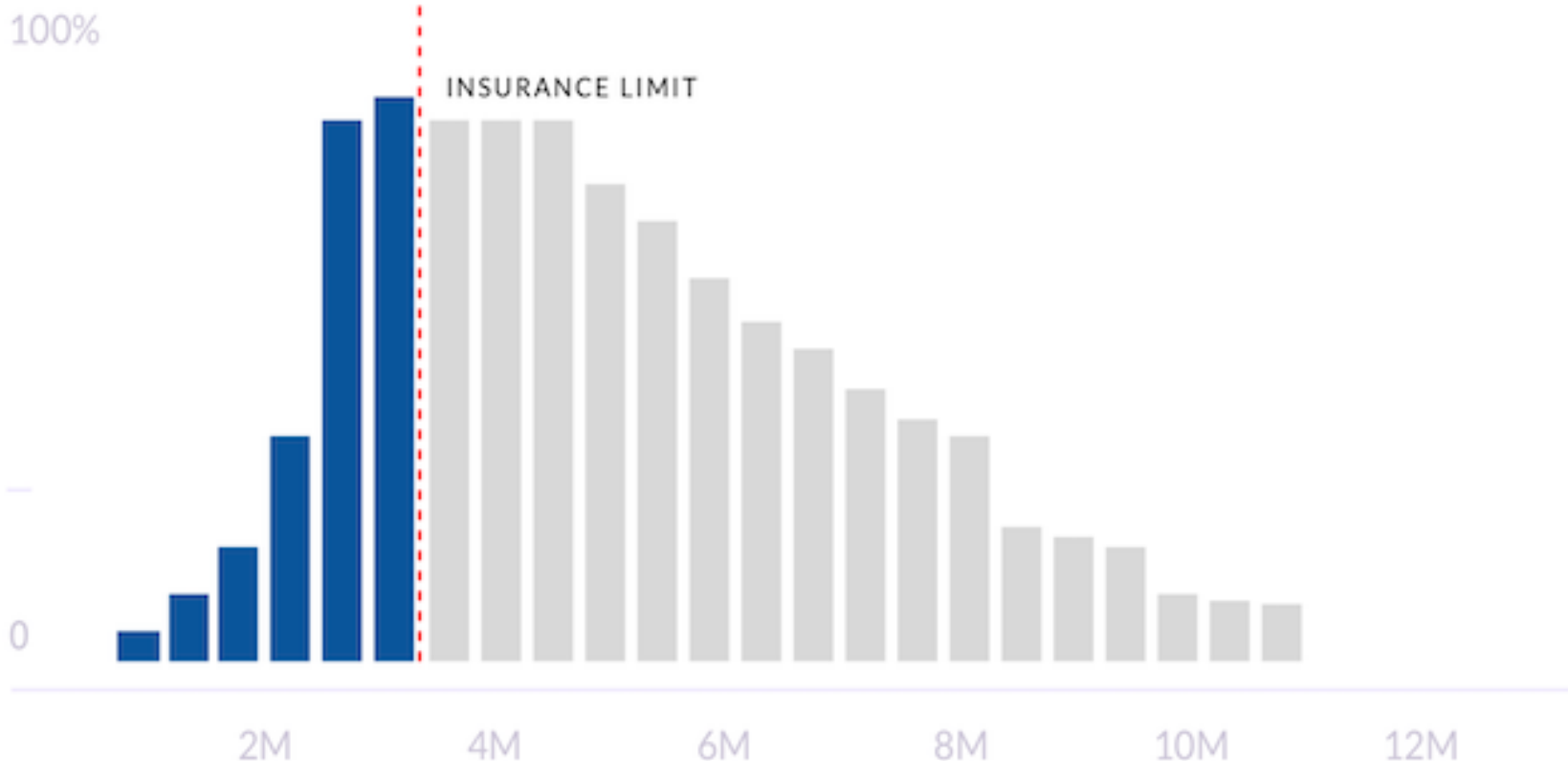


Ransomware - IT Servers and Endpoints

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 SUMMMARY

Calculation of Lost

$2M EXPECTED

$1M MIN

$4M MAX

Qualified of Imapcts

5

Impacts with Relevant Coverage

2

INSURANCE SUMMMARY

Total Coverage

$1.8M

Policy B Coverage

$700k

Policy C Coverage

$100k

Policy A Coverage

$1M

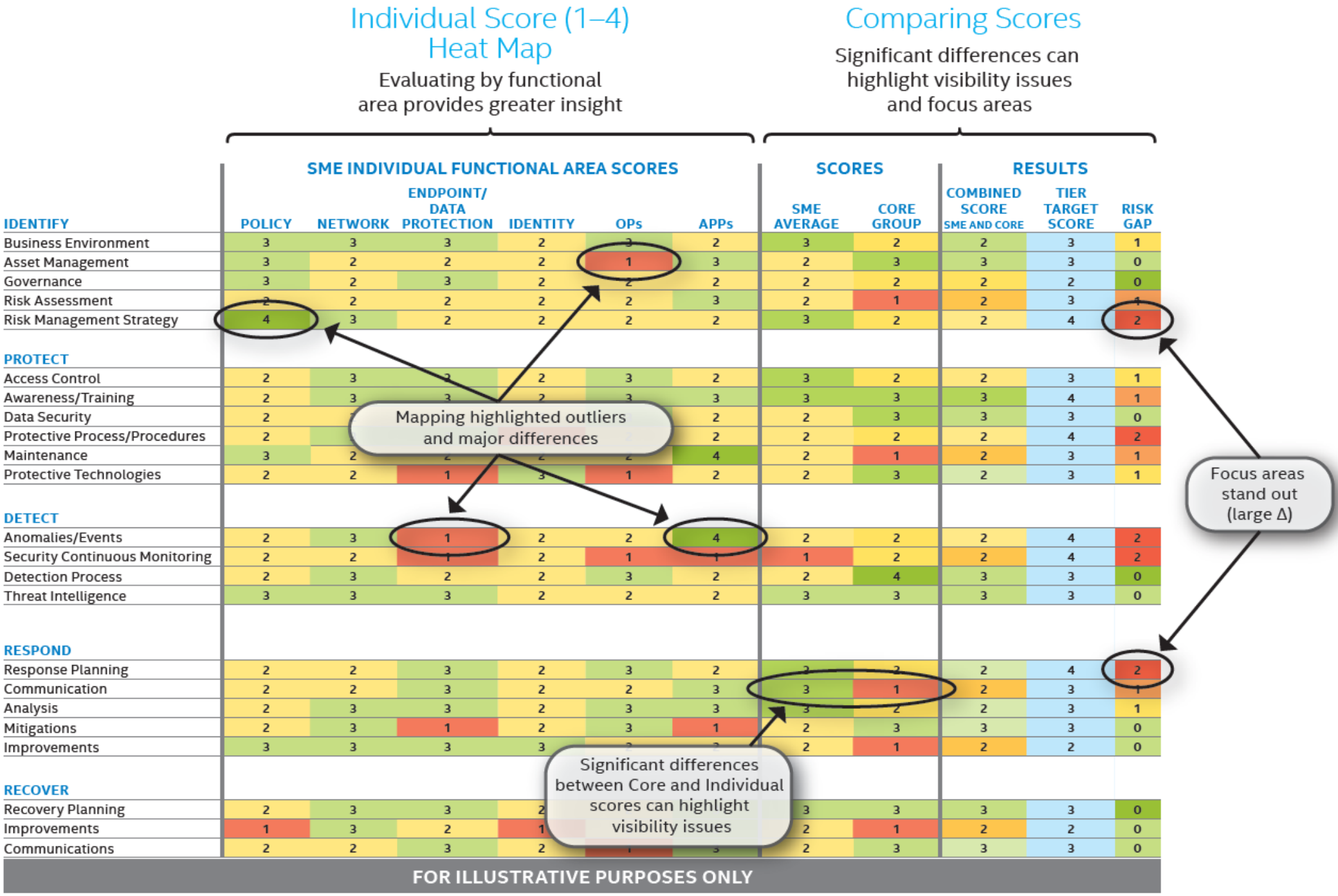
$200k UNCOVERED

Source: Axio

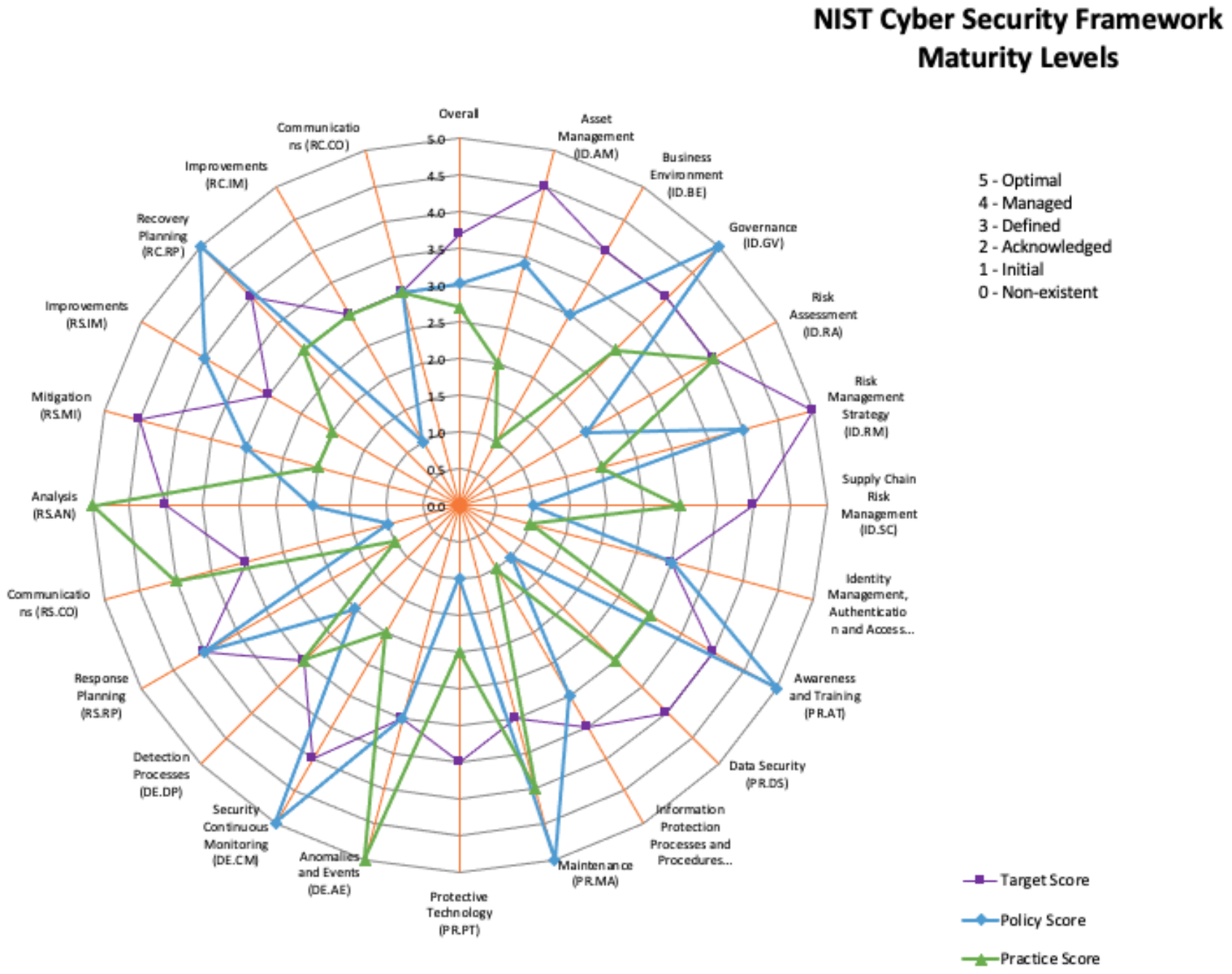
Process #3: Respond

Don’t put a $10 fence around a $5 horse.

Sample #1: CSF Target Profile Heat Map



Sample #2: CSF Target Profile Spider Chart

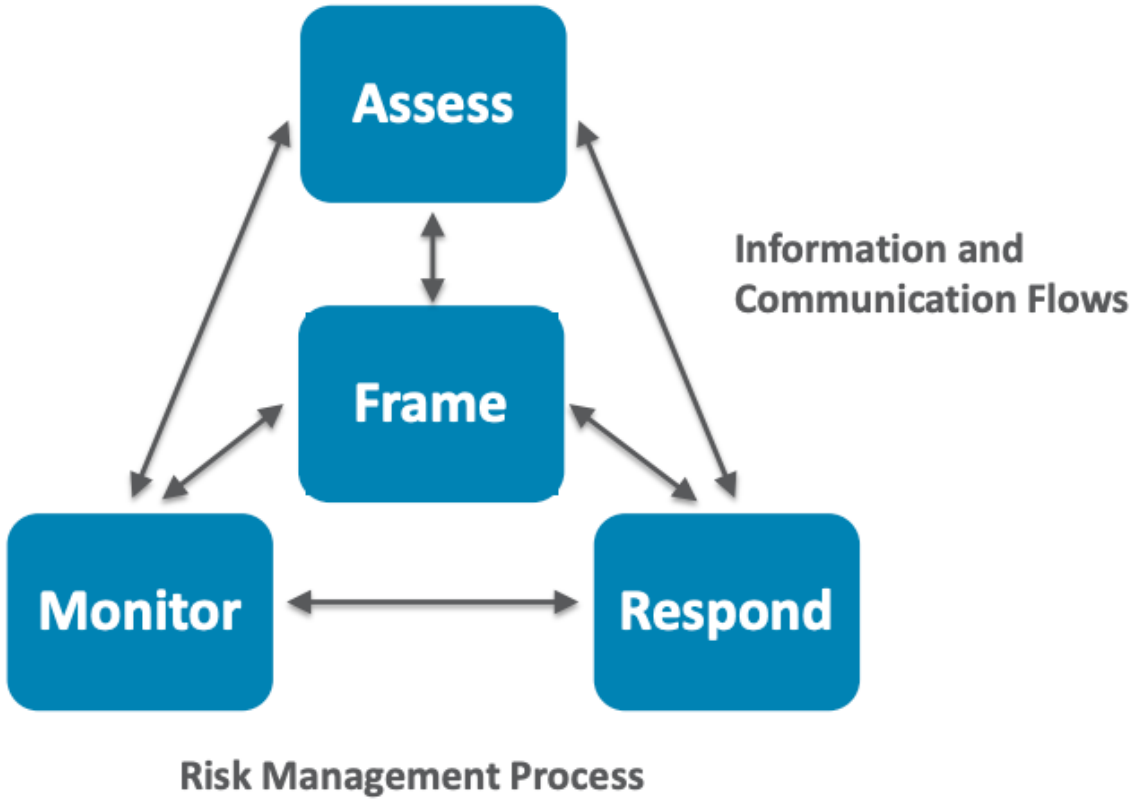


Process #4: Monitor

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											

Ref: NIST IR 8286

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@aretesolutions.com

DTHolland@cyberflorida.org