Unholy Concoction of Risk Management Practices: FAIR/CSF/MSSP

Ian Amit
Chief Security Officer, Cimpress

@iiamit

SIRACon 2019, May 2nd

Disclaimers

¯_(ツ)_/¯

IT WORKS

on my machine

First Grade

TRIGGER WARNING

EXPLICIT CONTENT

Brief Background

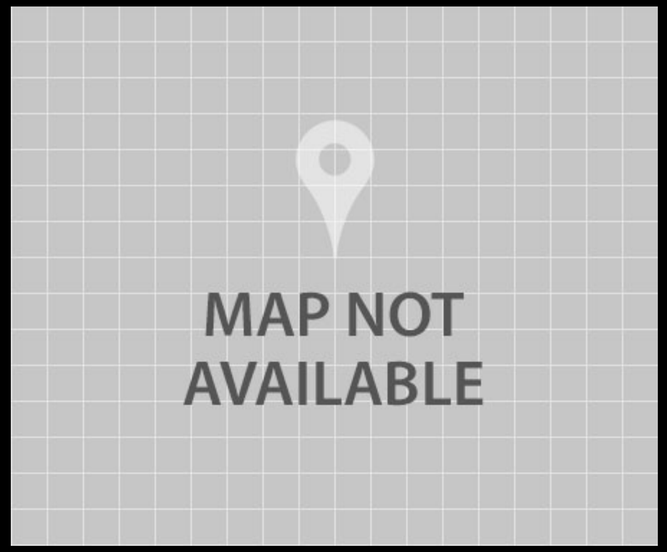
cimpress™

vistaprint

Challenges

Challenges


RULES
REGULATIONS
COMPLIANCE
STANDARDS
POLICIES


MAP NOT
AVAILABLE

Step 1: Mapping

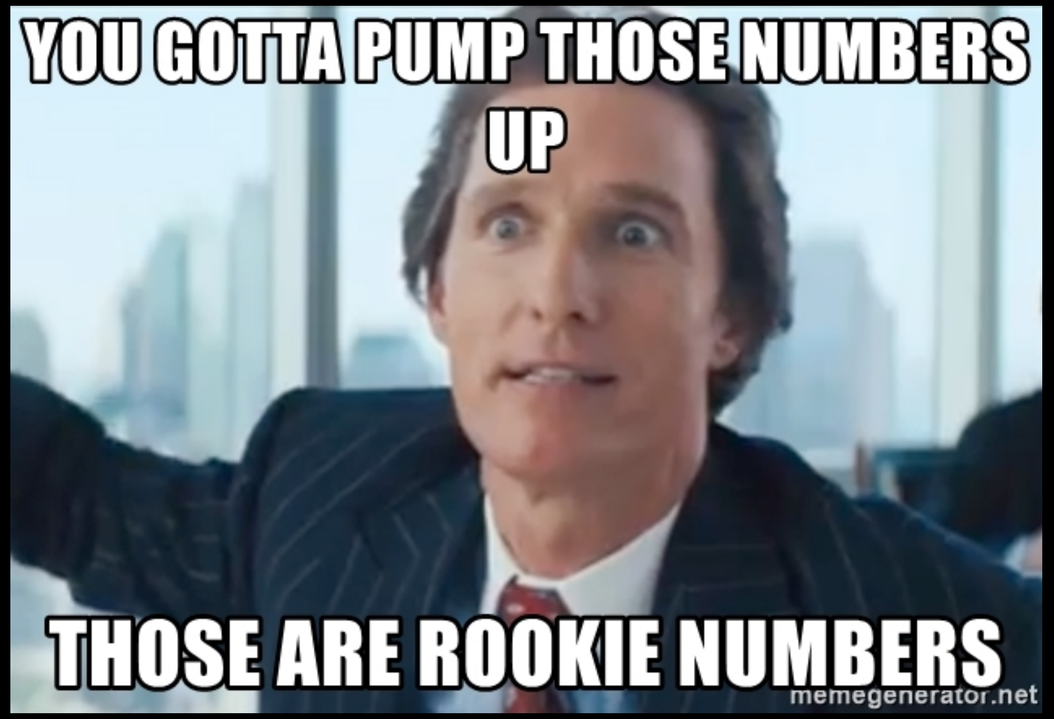
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond		
Recover		

NIST Framework	Initial	Partial	Repeatable	Adaptive
Process	No process	Processes are ad-hoc. Success is likely to depend on individual efforts	Consistent process and success can be repeated	Process measured and continually improved and introducing innovative processes to better serve the organization
Integration	No integration	Integration on system by system basis	Integration consistent, centralized, and throughout organization	Integration may be automated, orchestrated, or integrated via API
Sharing Information	No collaboration	Collaboration on an ad-hoc or project basis	Collaboration is consistent throughout the organization	Proactively shares information for stakeholders and partners to mitigate risk

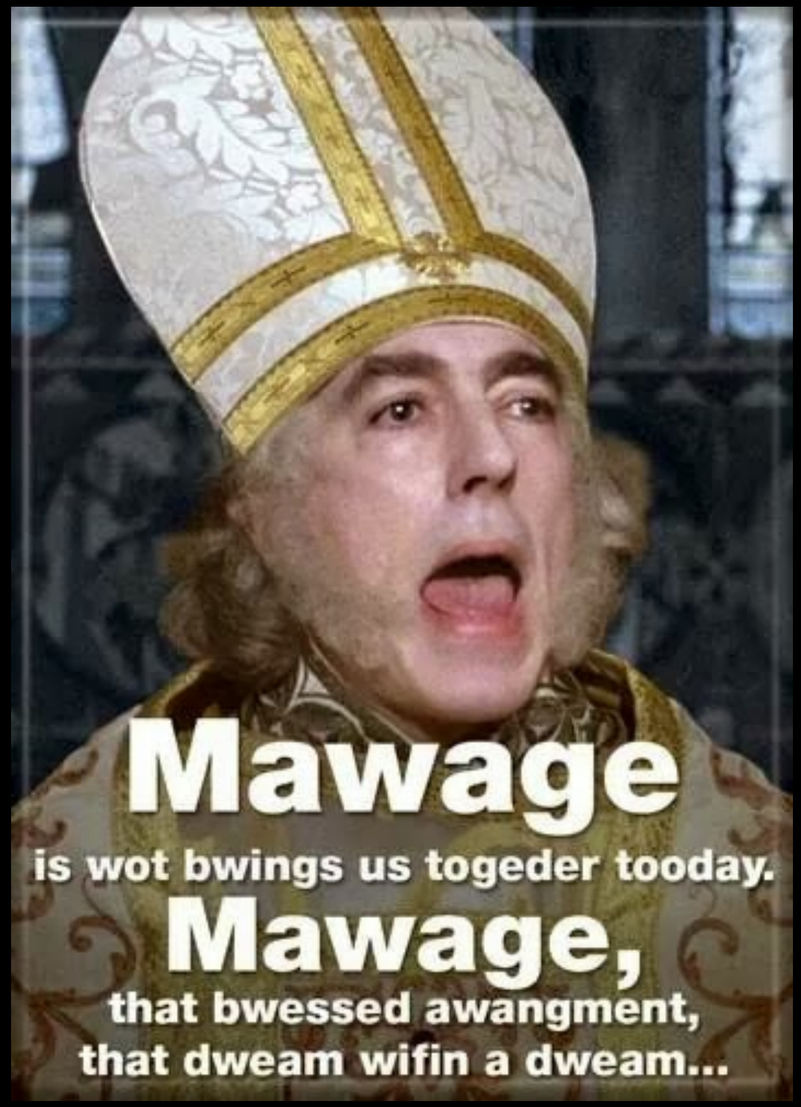
ID.AM-4: External information systems are catalogued	Initial - External information systems are not catalogued.	Partial - Some information may exist on organizational communication and data flows	Repeatable - The institution proactively manages system EOL (e.g., replacement) to limit security risks.	Adaptive - External information systems are proactively catalogued so attack surface to external information systems can be monitored and assessed.

Step 2: Risk


RISK
Loss Event Frequency
Loss Magnitude
Threat Event Frequency
Vulnerability
Primary Loss
Secondary Risk
Contact Frequency
Probability of Action
Threat Capability
Resistance Strength
Secondary Loss Event Frequency
Secondary Loss Magnitude
Random
Regular
Intentional
Value
Level of Effort
Risk
Skills
Knowledge
Experience
Resources
Time
Materials


YOU GOTTA PUMP THOSE NUMBERS UP
THOSE ARE ROOKIE NUMBERS
memegenerator.net

Step 3: Unholy Marriage



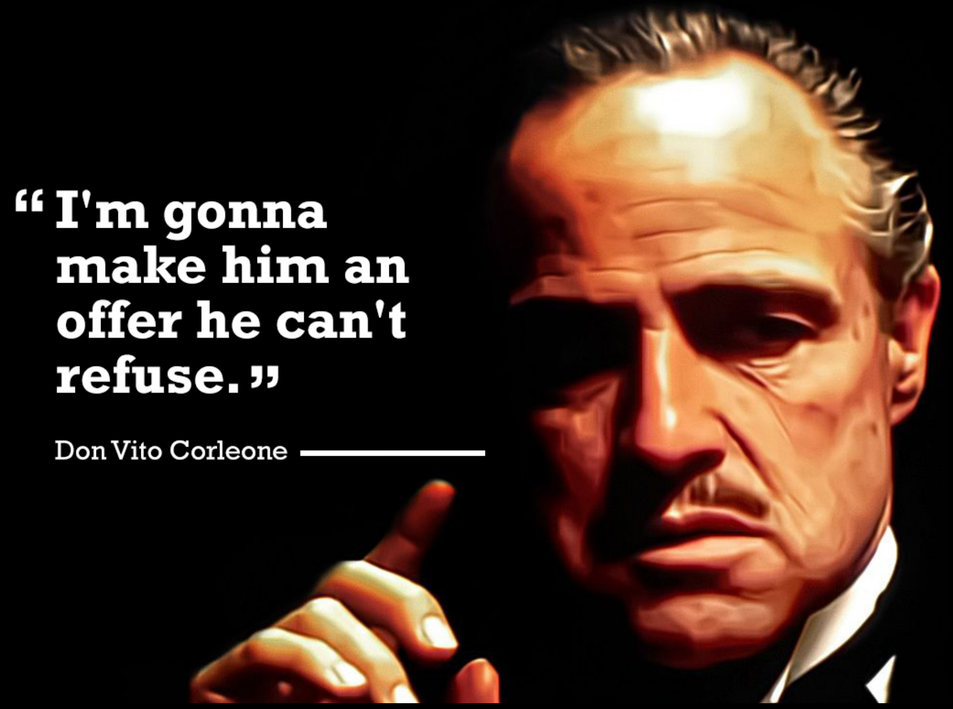
Resistance Strength	Cur.	Pro.
Min	50%	
ML	70%	
Max	80%	

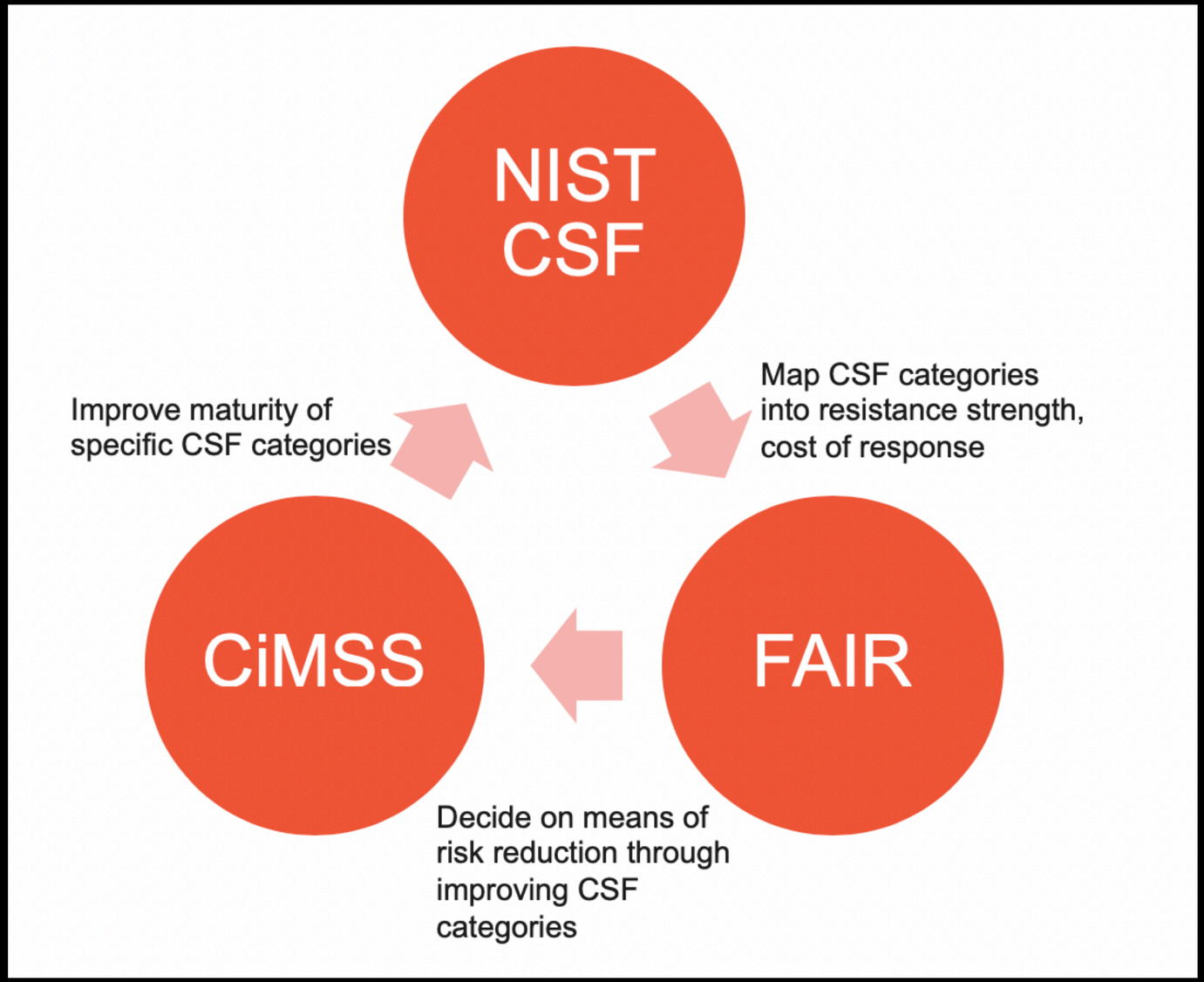
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	**Partial - Identity and credential policies are applied on an ad-hoc and project basis.**
		PR.AC-2: Physical access to assets is managed and protected	**Partial - Access controls exists on ad-hoc basis for physical assets that are not formalized.**
		PR.AC-3: Remote access (e.g.. Access from remote network, home, VPN) is managed	**Repeatable - Access controls for remote access is consistently applied to assets organization wide.**
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**Partial - Access permissions are applied to assets with or without regard to least privilege or separation of duties.**
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	**Partial - Network segments are created on ad-hoc basis if there is a requirement from a technical perspective.**

Recap

16 businesses X 3-5 loss scenarios
16 NIST-CSF scores

Step 4: Closing Gaps





TODO:

- Automate, automate, automate
  - CSF collection, processing, validation.
  - Mapping audits, pentests, control readings to CSF maturity levels.
  - CSF->FAIR: Still a subjective practice that's part of the discussion. No specific bell-curves to align to as highly scenario dependent.
- Baseline publishing - mapping policies, RFCs, regulations into ~30 sub-categories with defined minimum maturity levels.
  - Add baseline to Internal Audit ;-)
- Sub-business level measurements.
  - Per site? function? How to roll-up loss scenarios? How to roll up CSF scores?

Thank You!

Questions?