

Implementing the U.S. Cybersecurity Framework at Intel—A Case Study

Kent Landfield, Director Standards and Technology Policy



**How would you represent
your entire risk landscape to
your senior management?**



And how would you get there?

A Changing Landscape Drives Security



A security program must keep pace with the evolving threat landscape. It must become an intrinsic part of the enterprise that grows along with it.



US Cybersecurity Framework

What it is...

- An organizational Cybersecurity Risk Management **tool** for:
 - Improving communications between technical staff and the business decision makers
 - A common language for discussing organizational cybersecurity issues
 - Evaluating an organization's current security posture
 - Developing an organization's target security profile
 - Providing a means to develop a roadmap for improving the cybersecurity posture based on specifics
 - Improving Cybersecurity Risk Management decision making within the organization
- Voluntary
- Guidance created based on existing standards and best-practices (private and public sector were involved in the creation)
- A living document

Background

- Released (Version 1.0) February 12, 2014, it is in direct response and support of President Obama's February 2013 Executive Order 13636 "Improving Critical Infrastructure Cybersecurity."
- Helps organizations to identify, understand, manage and reduce cybersecurity risks by prioritizing security investments



NIST Cybersecurity Framework

What it is not...

- Prescriptive
- A replacement for existing risk management methodologies (but can augment and compliment OR fill gap if none exists)
- Foolproof! No, implementing the CSF does not mean you are immune to being compromised!
- A “One size fits all” approach
- A substitute for thoughtful review, evaluation and pragmatism in addressing risk concerns and priorities
- It is NOT an IT governance “Framework” in the classic sense of CoBIT
- It is not a silver bullet

Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

Source: *NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0.*

The Basics



CSF - Overview

The CSF provides a common method for organizations to:

1. Baseline and describe “as is” current posture

2. Describe “to be” target state

3. Identify and prioritize improvements

4. Assess progress

5. Communicate to stakeholders

CSF - Overview

Three primary components:

1) **Profile:** Comprised of two views; current “as is” and target “to be”

2) **Implementation Tiers (1 – 4):**
Partial, Risk Informed, Repeatable, Adaptive

3) **Framework Core:**

- Functions: Identify, Protect, Detect, Respond, Recover
- Categories, subcategories and Informative References

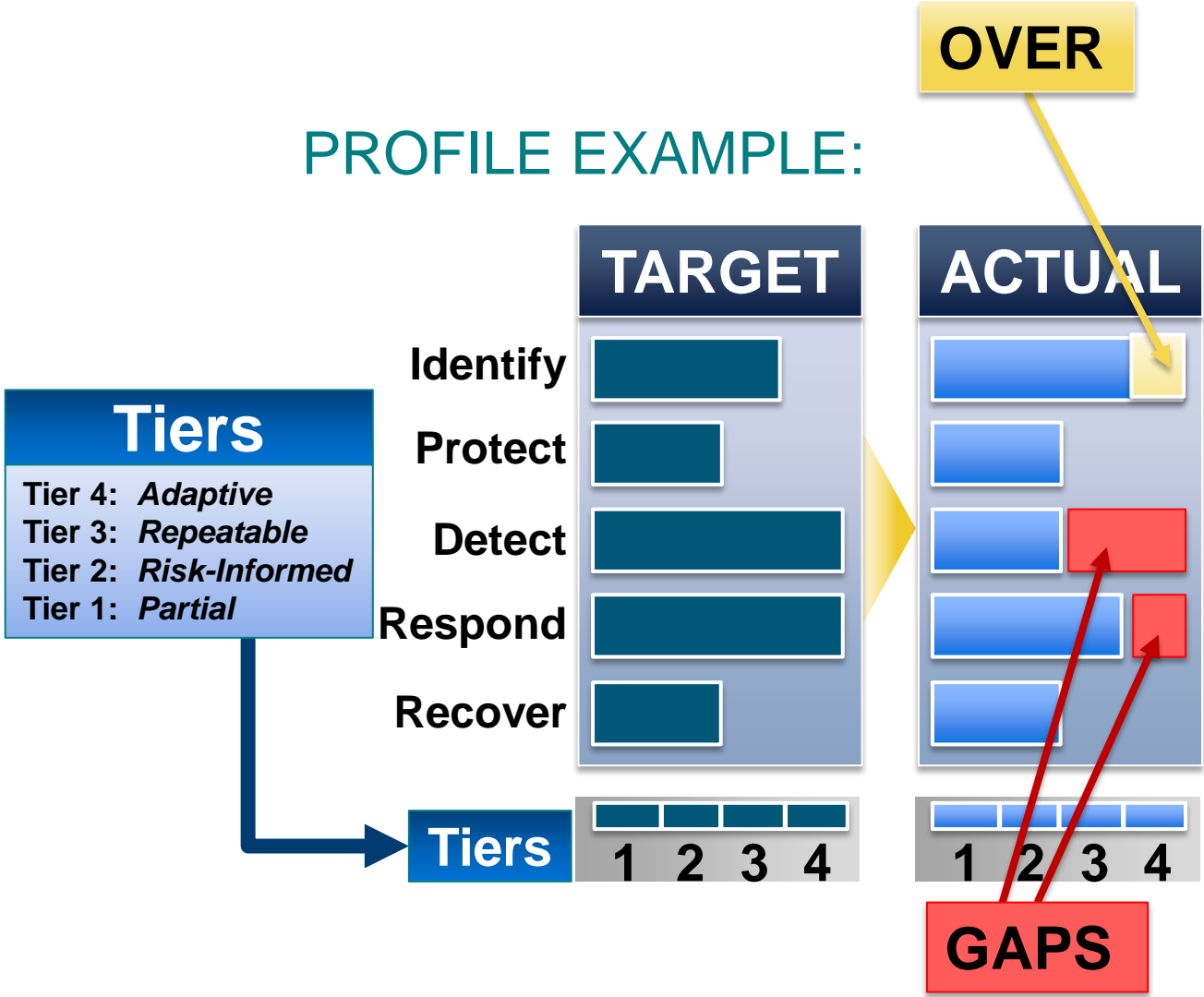
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Putting It Together

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Risk are assessed by Function Area with the ability to examine risks granularly through Categories/Sub Categories enumeration

PROFILE EXAMPLE:



- Tiers and Levels**
1. Organizations set Target Levels to match their Risk Tolerance
 2. Organizations examine their controls and assess gaps against Targets

Intel's Cybersecurity Framework Pilot

Laying the Groundwork

- Several methods to build comprehensive risk picture tried in the past, but none were satisfactory
- Intel actively involved with NIST and CSF from beginning (February 2013) and ready to pilot at release
- Team engaged and educated senior management at very beginning
- Also engaged other stakeholders early; their buy-in helped with resourcing
- Interestingly, the Framework itself facilitated the discussions



Intel's CSF Pilot Goals



Harmony of
Approach & Language



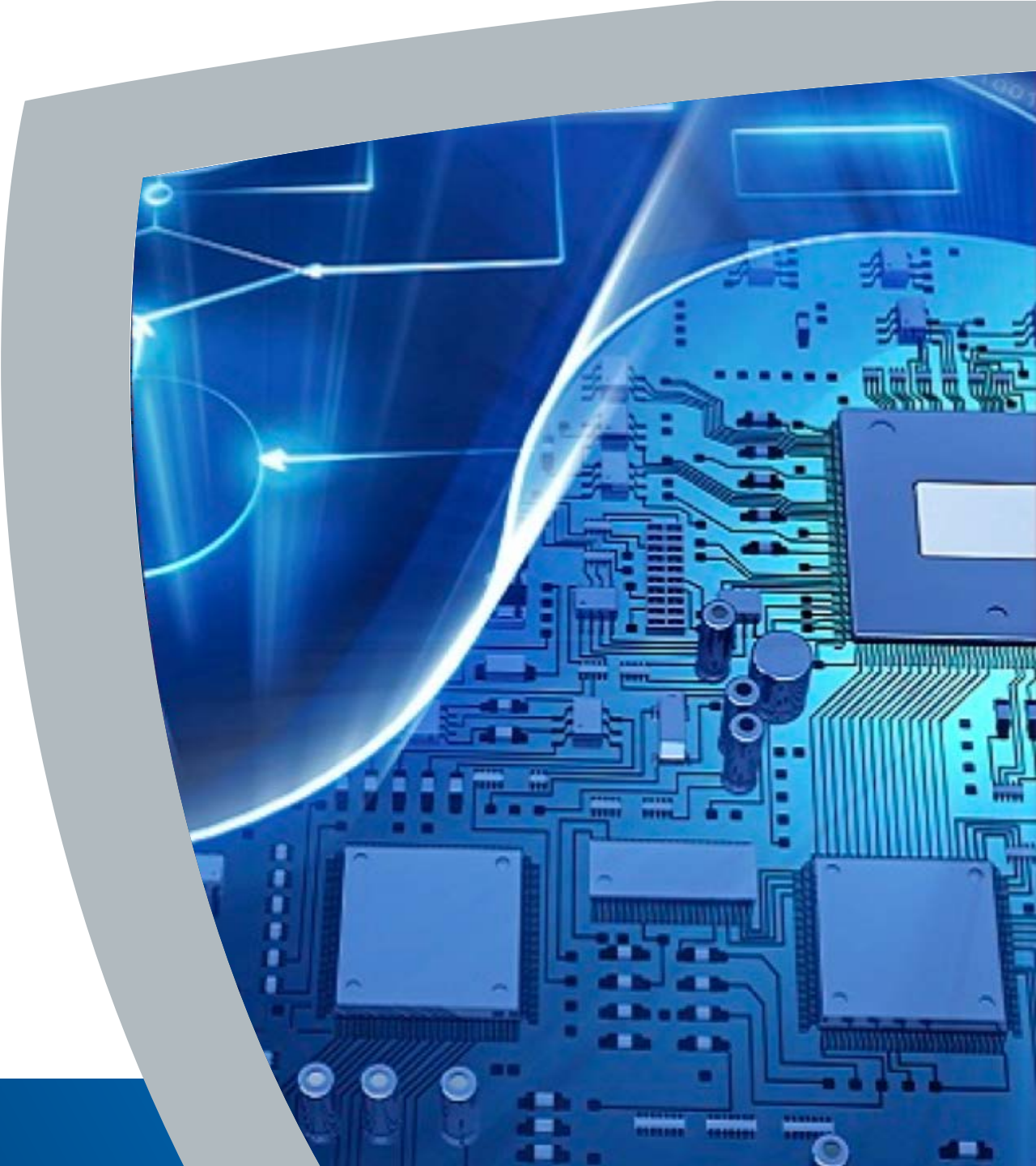
Right **Level** of
Cybersecurity



Informed
Budget Planning



Better **Communication**
to Leaders



Pilot Scoping – Subset of the Company

IT models support across the company as DOMES—Design, Office, Manufacturing, Enterprise, Services


Assessing entire enterprise with all subcategories too large a task for a pilot

Decided to only assess to **Category** level within **Office and Enterprise IT** domains

Our training covered how to assess within these constraints

	Design	Office	Manufacturing	Enterprise	Services
Identify					
Business Environment					
Asset Management					
Governance					
Risk Assessment					
Risk Management Strategy					
Protect					
Access Control					
Awareness/Training					
Data Security					
Protective Process & Procedures					
Maintenance					
Protective Technologies					
Detect					
Anomalies/Events					
Security Continuous Monitoring					
Detection Process					
Threat Intelligence					
Respond					
Response Planning					
Communication					
Analysis					
Mitigations					
Improvements					
Recover					
Recovery Planning					
Improvements					
Communications					

Focus Areas



Tiers – People, Process, Technology & Ecosystem

		Score 1 - Partial	Score 2 – Risk Informed	Score 3 - Repeatable	Score 4 - Adaptive
1					
2	People	Staff has had minimal cybersecurity-related training. There is limited or non-existent training pipeline for security staff. Security awareness is limited. Staff has non-existent or limited awareness of Intel Security resources and escalation paths.	Employees have received cybersecurity-related training. There is a training pipeline for security staff and personnel. There is an awareness of cybersecurity risk at the organizational level. Employees have a general awareness of security and Intel Security resources and escalation paths.	Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. Employees receive regular cybersecurity-related training and briefings. There is a robust training pipeline for security staff and personnel. Employees attend internal and external security conferences or training opportunities. Organization has a Security Champion or dedicated security personnel.	People: Personnel knowledge and skills are regularly reviewed for currency and applicability and new skills and knowledge needs identified and addressed... Employees receive regular cybersecurity-related training and briefings on relevant and emerging security topics. There is a robust training pipeline for security staff and personnel. Employees routinely attend internal and external security conferences or training opportunities.
3	Process	Risk management process not formalized; Risks are managed in a reactive, ad hoc manner. Business decision and/or prioritization do not factor in risk and/or threat assessments. Risk and threat information is not communicated to internal stakeholders.	approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis. Risk management practices are approved by management but may not be established as organizational-wide policy.	technology landscape. Risk management practices are formally approved and expressed as policy and there is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk.	The organization adapts its cybersecurity practices based on lessons learned from active indicators derived from previous and current cybersecurity events. Through a process of continuous improvement incorporating cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
4	Technology	Tools are not deployed, not supported or insufficient to address risks. Tools may be in place but are not adequately tuned or maintained. Technology deployed lags current threats. Tool coverage lacking (tool is deployed in a limited way).	Tools are deployed and supported to address identified risks. Tools in deployment are routinely tuned and/or maintained. Technology deployed, for the most part, paces current threats. Tool coverage of the risk area is complete.	Metrics are used to evaluate the usefulness and effectiveness of deployed tools. Tools in deployment are tuned and/or maintained. Technology deployed paces current and emerging threats. Tool coverage of the risk area is complete and as new infrastructure is deployed, tool coverage is addressed.	Tools deployed in the environment are regularly reviewed for effectiveness and coverage against changes in threat environment and internal ecosystem. Tools and technology deployed anticipates emerging threats.
5	Ecosystem	Organization does not know its role in the larger ecosystem. Organization does not have processes in place to participate in or collaborate with external organizations.	The organization knows its role in the larger ecosystem but has not formalized its capabilities to interact and share information externally.	The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

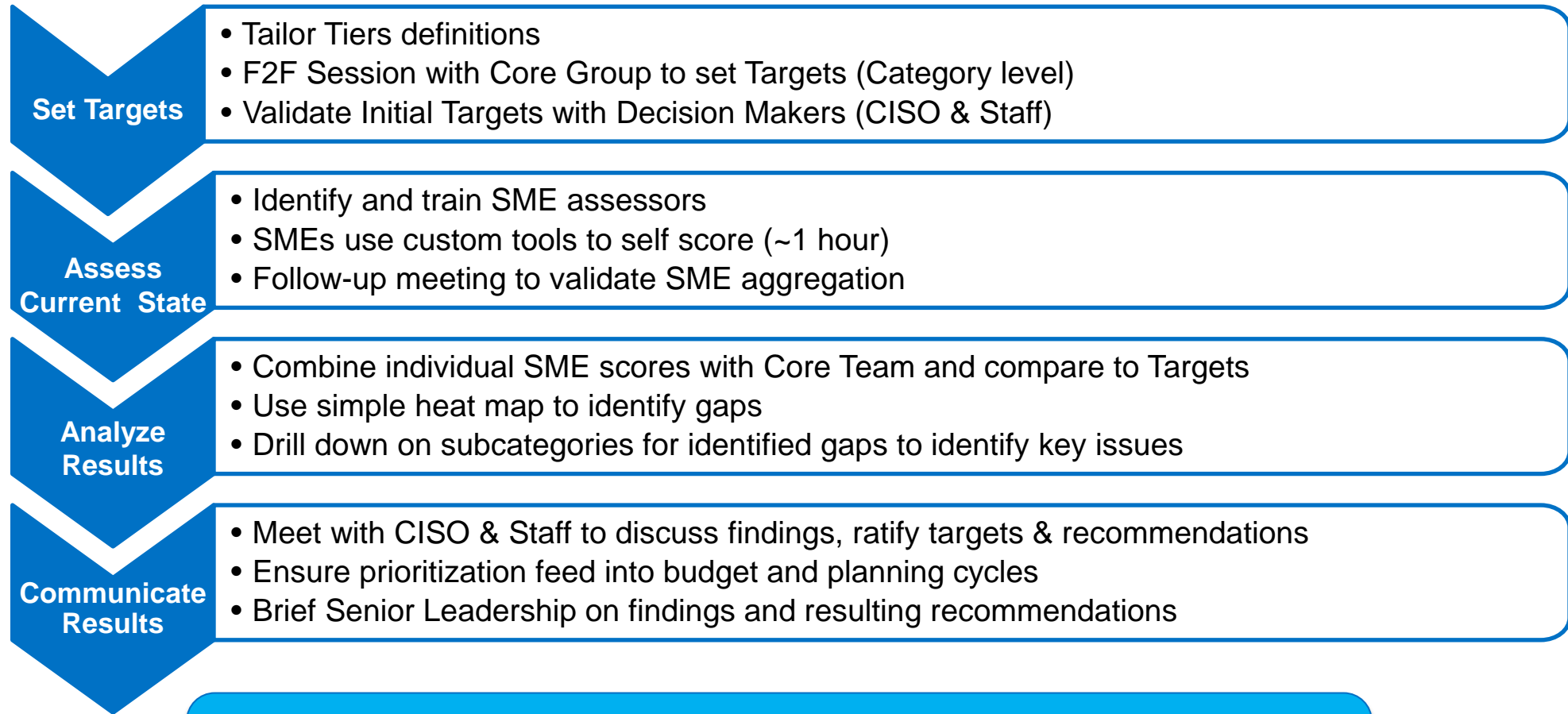
Overall: Tiers Definitions worked well for participants

Need to harmonize wording (staff, personnel, etc.)

Need to refine 'seams' between Tiers

Need to clarify scope of dimension quality when using in categories

Framework Utilization Process



Intel's white paper details all these steps.

CSF – Outcomes and evolution - examples

SME roll-up of self-assessment (current profile against top-level categories) – outliers and differences (gaps):

	Policy	Network	Endpoint/ Data Protection	Identity	Ops	Apps	SME Ave
Identify							
Business Environment	3	3	3	2	3	2	3
Asset Management	3	2	2	2	1	3	2
Governance	3	2	3	2	2	2	2
Risk Assessment	2	2	2	2	2	3	2
Risk Management Strategy	4	3	2	2	2	2	3
Protect							
Access Control	2	3	3	2	3	2	3
Awareness/Training	2	3	3	2	3	3	3
Data Security	2	2	2	2	3	2	2
Protective Process and Procedure	2	3	3	1	2	2	2
Maintenance	2	2	2	2	2	4	2
Protective Technologies	2	2	1	3	1	2	2
Detect							
Asset Monitoring	2	3	1	2	2	4	2
Threat Intelligence	2	2	1	2	1	1	1
	2	3			3	2	2
Respond							
Response Planning	2	2	3	2	3	2	3
Communication	2	2	3	2	2	3	3
Analysis	2	3	3	2			
Mitigations	2	3	1	2			
Improvements	3	3	3	3	2	2	2
Recover							
Recovery Planning	2	3	3	2	2	3	3
Improvements	1	3	2	1	2	3	2
Communications	2	2	3	2	1	3	2

Highlight outliers

Highlight major differences

EXAMPLE ONLY

NOTION

CSF – Outcomes and evolution - examples

Results! Again, this in turn can be used for further strategic prioritization, resource investment and deeper assessment against specific and desired outcomes

NOTIONAL / EXAMPLE ONLY

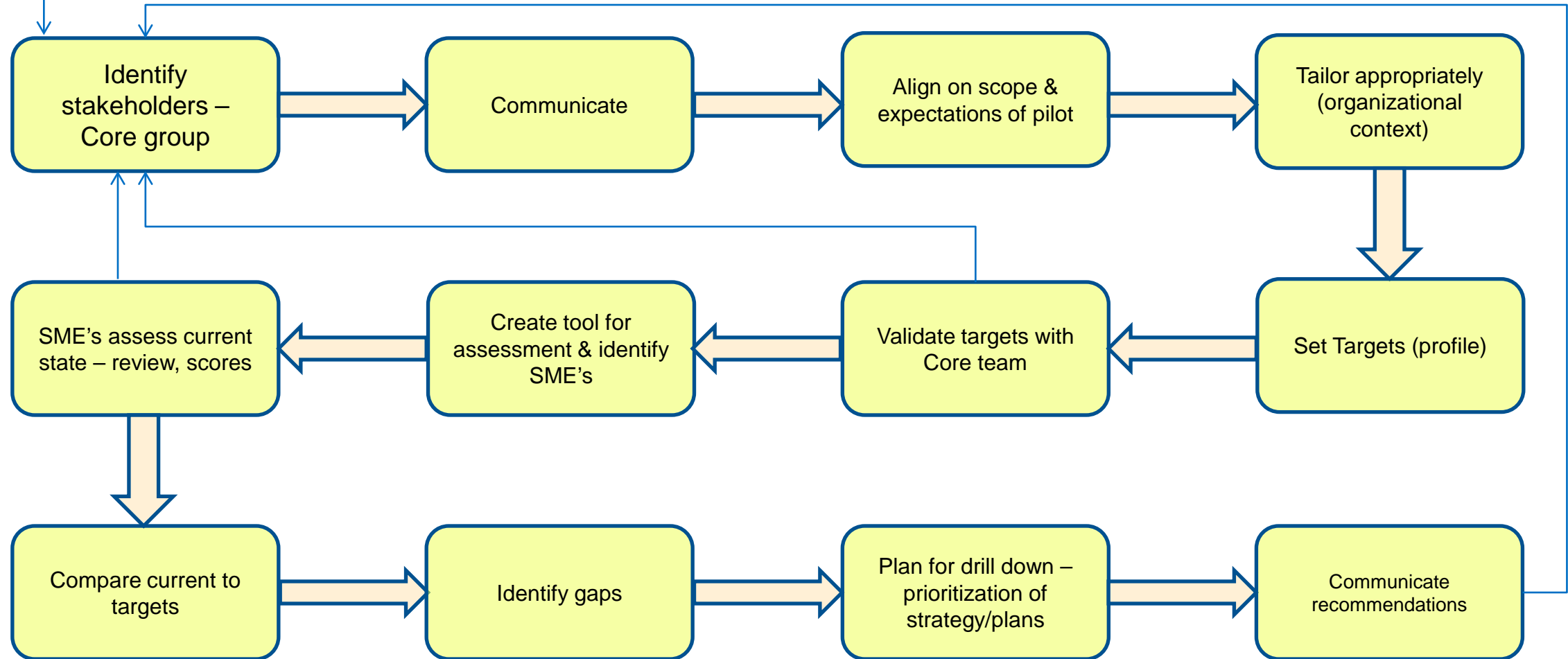
Category	Actual	Target	Delta
Identify	3	3	0
Business Environment	2	2	0
Asset Management	2	2	0
Governance	4	3	1
Risk Assessment	2	2	0
Risk Management Strategy	2	4	-2
Protect	2	2	0
Access Control	1	1	0
Awareness/Training	2	3	-1
Data Security	2	2	0
Protective Process & Procedures	2	2	0
Maintenance	3	4	-1
Protective Technologies	2	2	0
Detect	1	1	0
Anomalies/Events	3	2	1
Security Continuous Monitoring	4	4	0
Detection Process	2	2	0
Threat Intelligence	3	4	-1
Respond	2	2	0
Response Planning	1	1	0
Communication	3	3	0
Analysis	2	2	0
Mitigations	2	2	0
Improvements	3	4	-1
Recover	3	3	0
Recovery Planning	2	4	-2
Improvements	2	2	0
Communications	4	4	0



Summary

CSF – Methods and ideas for alignment

Start small - think BIG:



Looking Ahead: Insider Risk and CSF

Attack Type ↓	Non-hostile			Non-Hostile / Hostile		Hostile							
	Reckless Employee	Untrained/Distracted Employee	Outward Sympath'zr	Vendor	Partner	Irrational Individual	Thief	Disgruntled Employee	Activist	Terrorist	Organized Crime	Competitor	Nation State
Accidental leak	X	X	X	X	X	X		X					
Espionage				X	X		X	X	X		X	X	X
Financial fraud				X	X		X	X			X		
Misuse	X	X	X	X	X	X		X	X				
Opport. data theft				X	X		X	X	X		X	X	X
Physical Theft						X	X	X		X	X		
Product alteration	X	X		X	X			X	X		X	X	X
Sabotage						X		X	X	X		X	X
Violence						X		X		X			

Intel Threat Agent analysis of most-likely insider threats in a typical corporate environment

Goal: Pilot using CSF to assess and characterize our Insider Risk

Utilizing the CSF in Your Organization

You will miss the benefits if you treat the Framework as a compliance exercise, or use an outside agency do it for you

→ Coaching is fine but *you need to make the journey yourself*

1. Inform senior management on the Framework and benefits
2. Engage and inform all your stakeholders
3. With the stakeholders, design your pilot & set Tiers
4. Execute the pilot



Pilot Recommendations

Recommend pilot of top level (categories) as starting point which will allow for:

- Identifying critical gap areas for further strategic investment, prioritization and focus
- Minimize getting bogged down by going too deep out of gate
- Create a consistent dialogue and vernacular within the organization relative to risk management and risk-posture baseline
- Crawl – Walk – then Run! Set expectations and align the organizational context to the CSF to maximize its use and benefit
- Starting point to better understand and articulate the complete risk picture across the organization
- Wash, rinse...repeat. Lessons will be learned along the way. Make adjustments and keep the communication channels open

Our Key Learnings

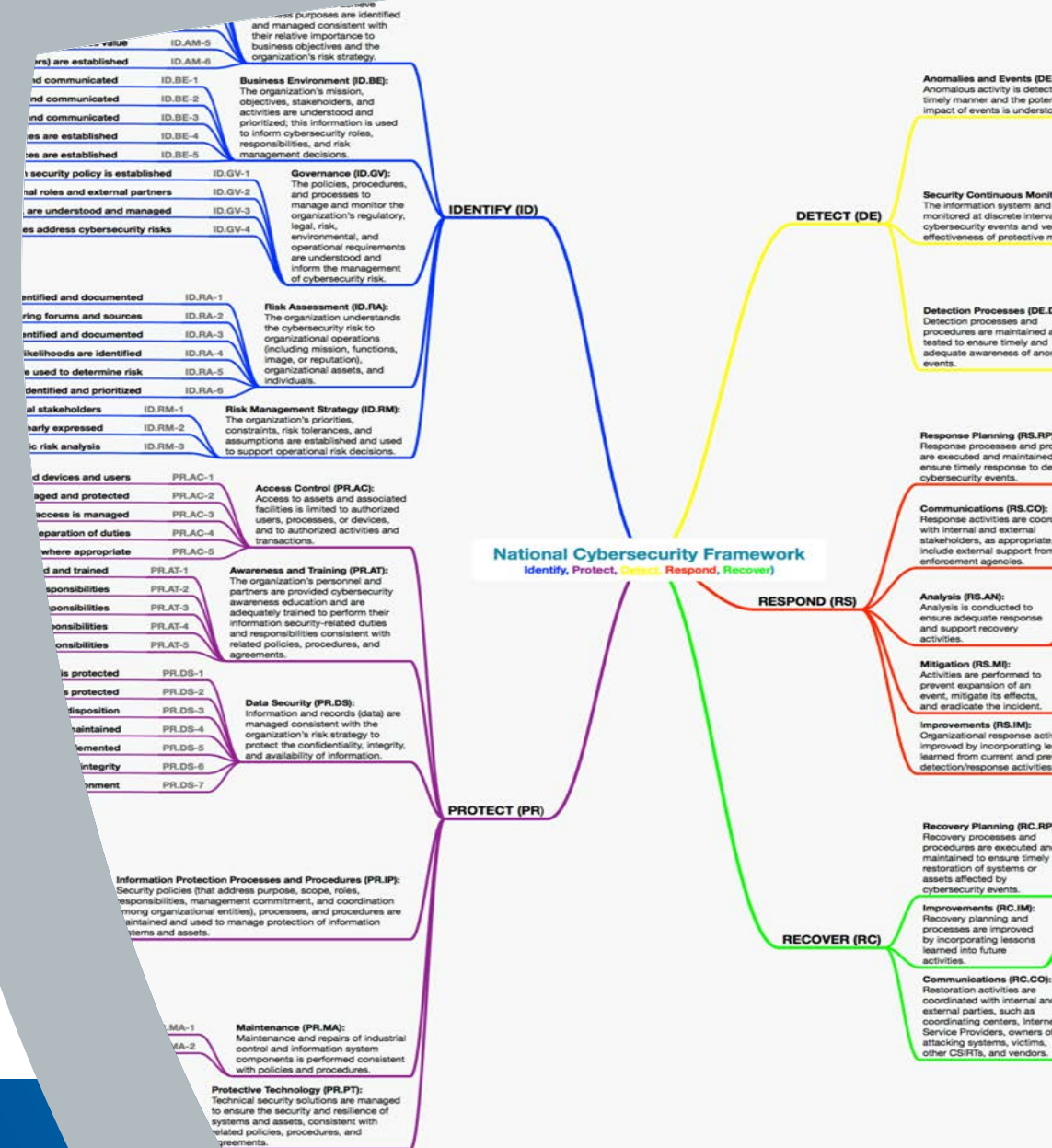
The CSF fosters essential internal discussions about alignment, risk tolerance, control maturity, and other elements of cyber risk management

- Setting our own Tier Targets was especially useful

The CSF provides a common language for cross-organizational communications, allowing apple-to-apples comparisons

Engage all stakeholders early; the Framework itself facilitates discussion

Its alignment to industry practices made it easy to scale and tailor it to our environment with surprisingly minimal impact



Additional Resources

Intel CSF white paper: <http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html>

NIST CSF Website: <http://www.nist.gov/cyberframework>

U.S. Sector Information Sharing & Analysis Centers (ISAC): <http://www.isaccouncil.org/home.html>

U.S. Dept. Homeland Security Critical Infrastructure Cyber Community (C³) Voluntary Program: <http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program>

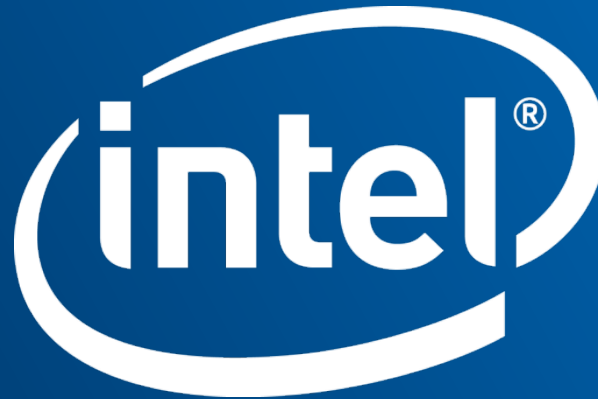
Intel Insider Threat Analysis: <http://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/a-field-guide-to-insider-threat-paper.html>

We actively engage with fellow travelers and communities utilizing the CSF related to:

- ◆ Threat Assessments
- ◆ Supplier Management and Supply Chain Risk
- ◆ Manufacturing / ICS Risk
- ◆ Tools and Visualization

Questions?





This presentation is for informational purposes only.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS AND SERVICES. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS AND SERVICES INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Intel, the Intel logo, Look Inside., and the Look Inside. logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2015 Intel Corporation. All rights reserved.