

ISACA Work on Standards and Frameworks

Recent Activities from Several Viewpoints

Greg Witte, CISSP-ISSEP, CISM
Greg.Witte@g2-inc.com
ManageTheRisk.com

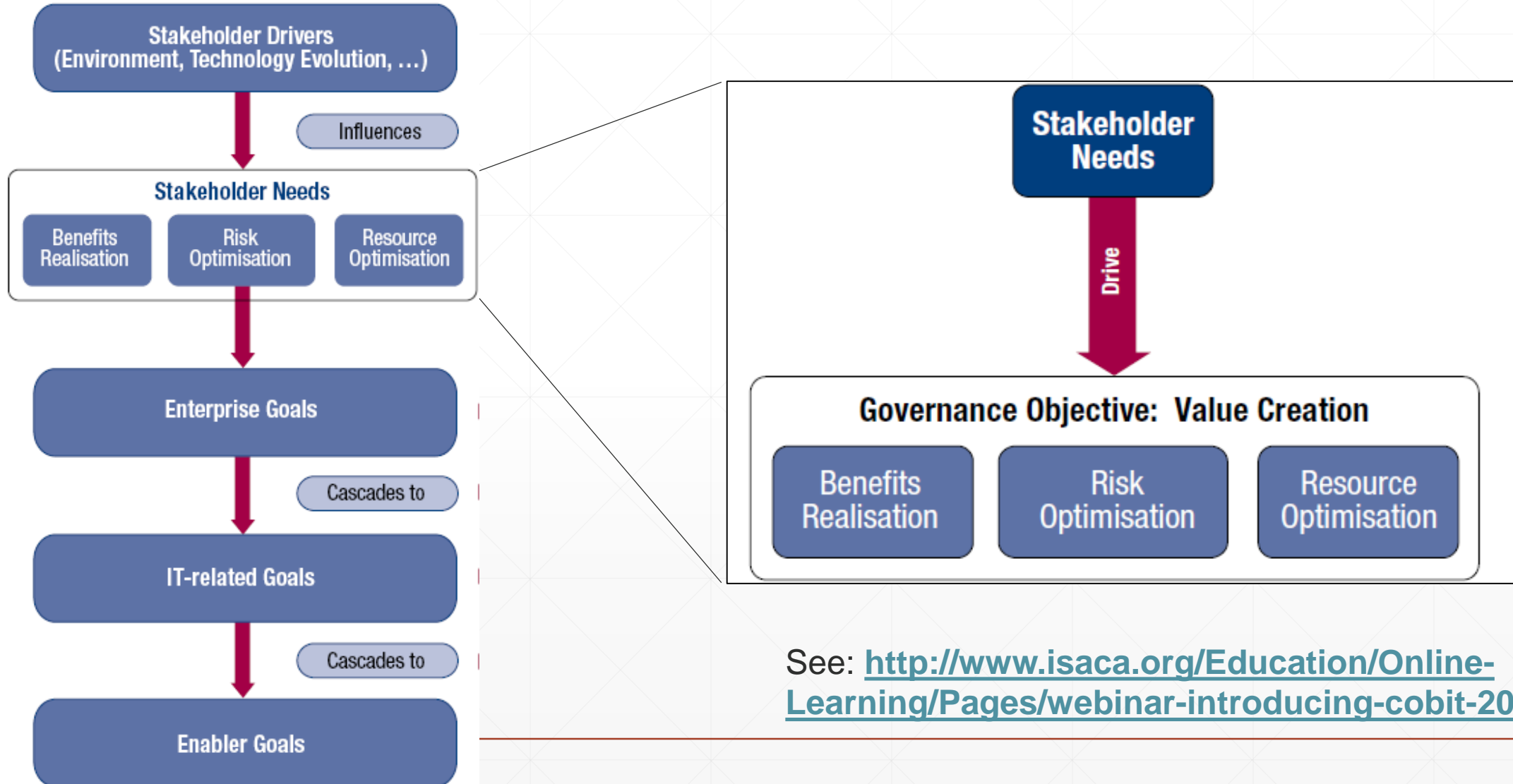


ISACA is there for you, wherever you are!



- Global, not-for-profit consortium of security-minded individuals, sharing info since 1969
- 140,000 members in 200 chapters throughout 180 countries
- Education, certification, resource sharing, advocacy, professional networking

ISACA provides critical links between business and cybersecurity aspects, including CTI



See: <http://www.isaca.org/Education/Online-Learning/Pages/webinar-introducing-cobit-2019.aspx>

ISACA works closely with the U.S. National Institute of Standards and Technology

- I don't speak **for** NIST, but pleased to speak **about** NIST's great work
- NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
- Agency of U.S. Department of Commerce, originated in 1901



Advanced Manufacturing



IT and Cybersecurity



Healthcare



Forensic Science



Disaster Resilience



Cyber-physical Systems




Advanced Communications

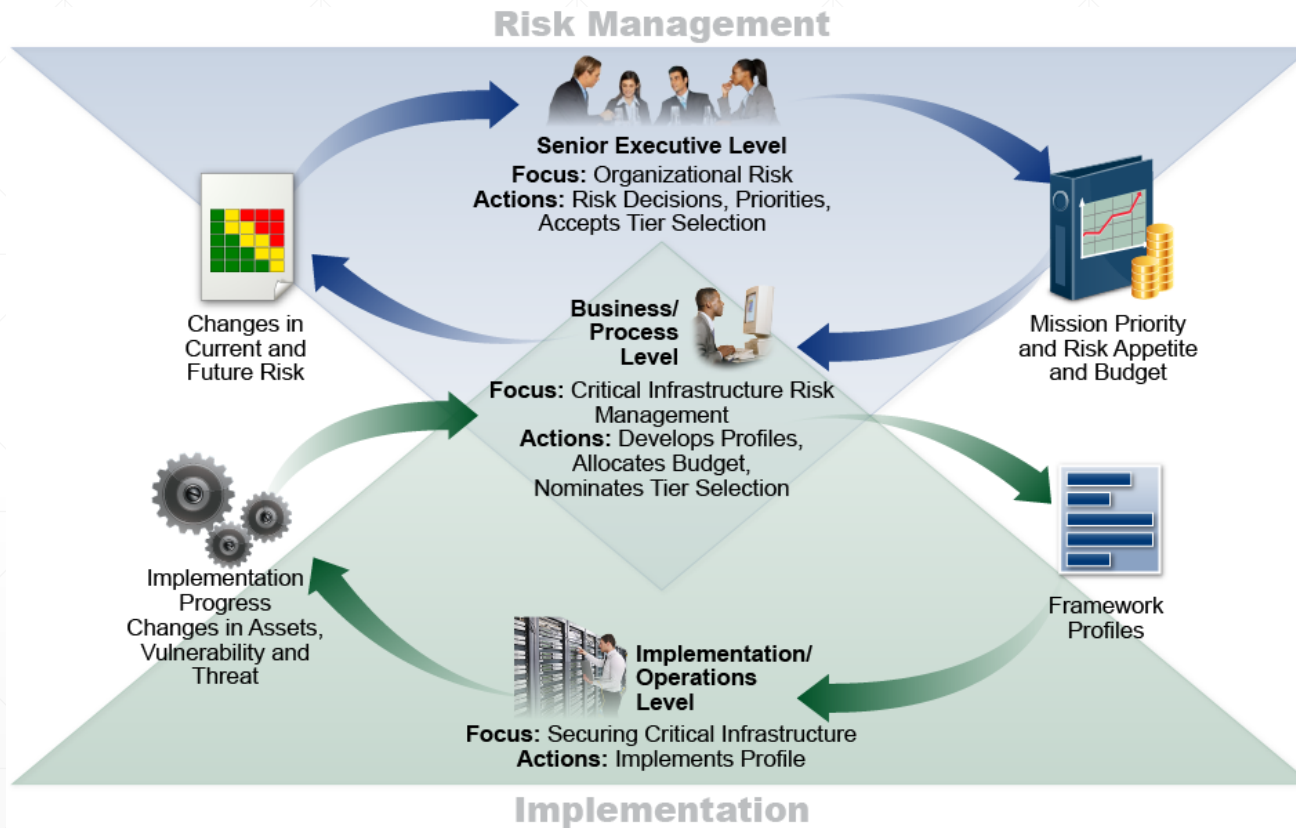
Audience Poll:

How many here are using
the NIST Framework?

ISACA Contributes to Many Relevant NIST Frameworks including:

- Cyber-Physical Systems (CPS) Framework
- Baldrige Excellence Framework
- Framework for Improving Critical Infrastructure Cybersecurity (or the Cybersecurity Framework)
- Risk Management Framework
- NICE Framework (Workforce)
-  Privacy Framework

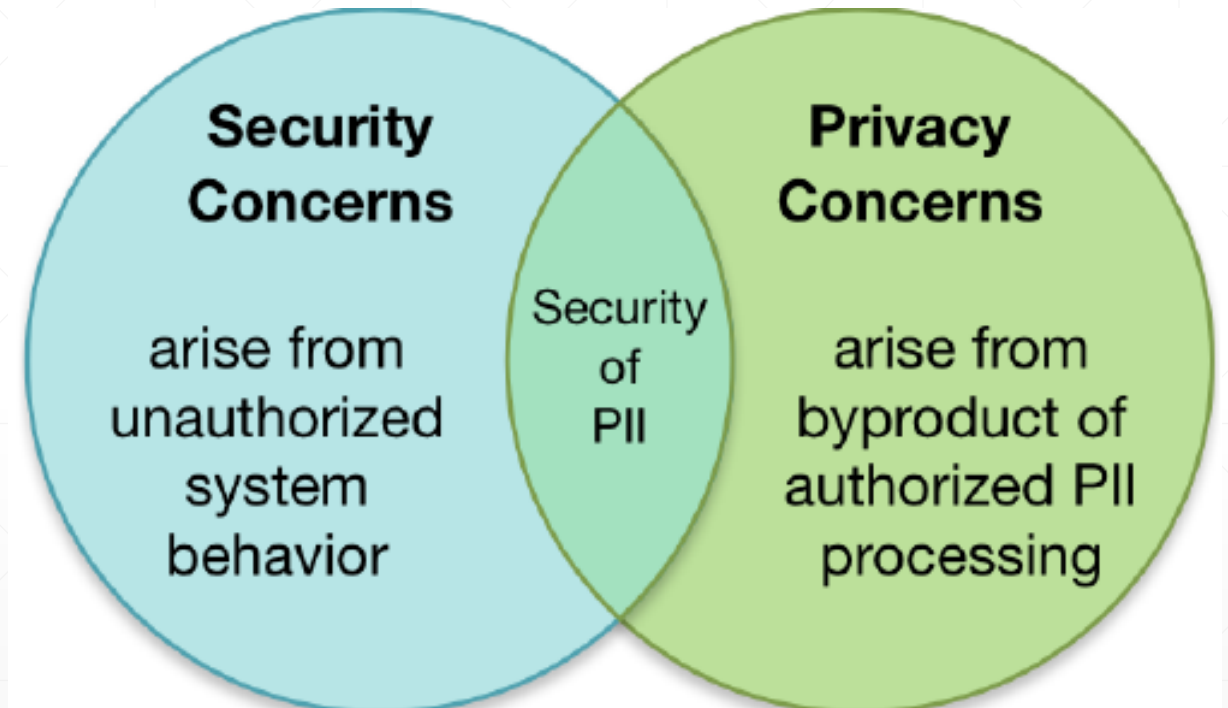
We Helped Create the Cybersecurity Framework



See: <https://www.nist.gov/cyberframework/online-learning>

ISACA will also Support NIST's New Privacy Framework

- Development of trustworthy information systems by –
 - applying measurement science
 - system engineering principles
 - to the creation of frameworks, risk models, guidance, tools, and standards
 - that protect privacy and, by extension, civil liberties.



See: <https://www.nist.gov/privacy-framework>

Challenges of a Voluntary Approach



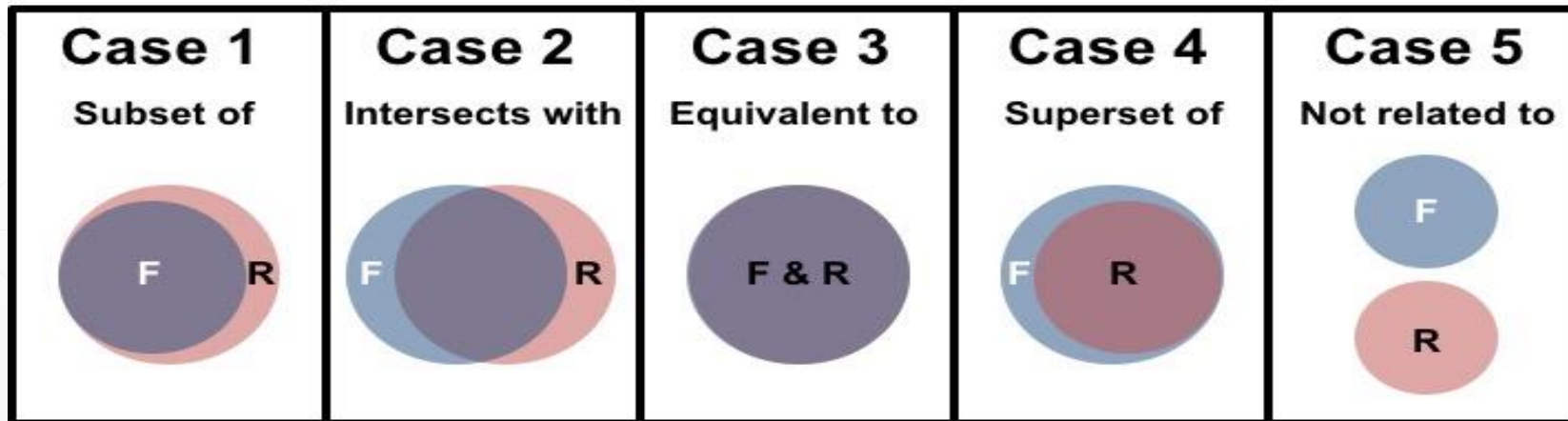
- Many commenters continue to request that the Frameworks remain voluntary
- Many organizations want to do the right thing but need a flexible approach

- Effective pressure to “do the right thing”
- We often hear concerns from organizations that want assurance that they are doing “enough”, both for their own due diligence and also to avoid penalties



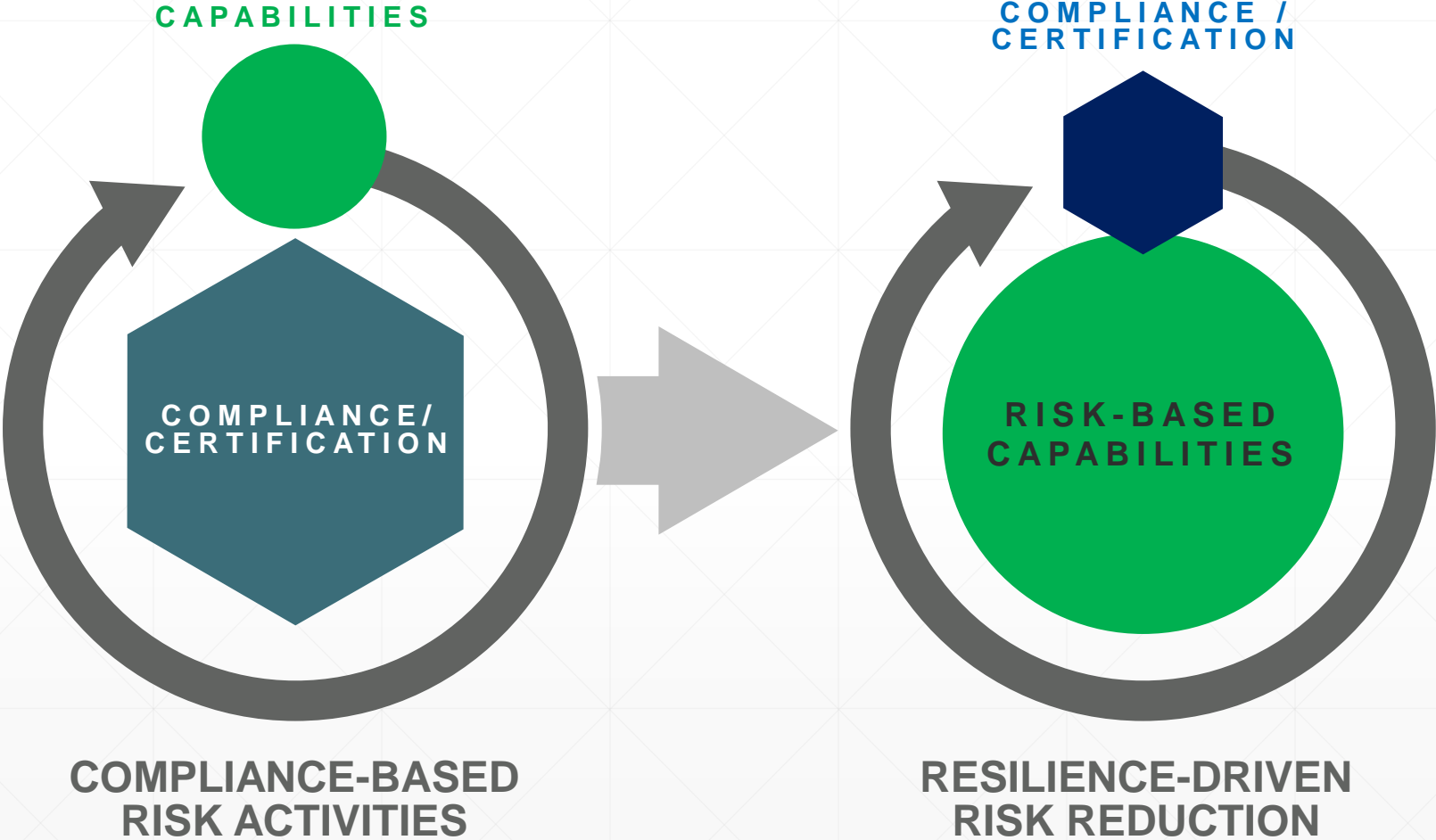
NIST is Updating Mappings and Informative References Including Those to COBIT

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27001:2013	NIST CYBER SECURITY FRAMEWORK	ISA/IEC 62443 3-3
Part 1 – Governance and Ecosystem					
1.1	Information System Security Governance & Risk Management	Information system security risk analysis	# 8.2 Information security risk assessment (ISO 27001) # 8.3 Information security risk treatment (ISO 27001)	ID.GV-4 ID.RA-1,2,3,4,5,6 D.RM-1,2,3 PR.AT-2	SR 5.2, 5.3,

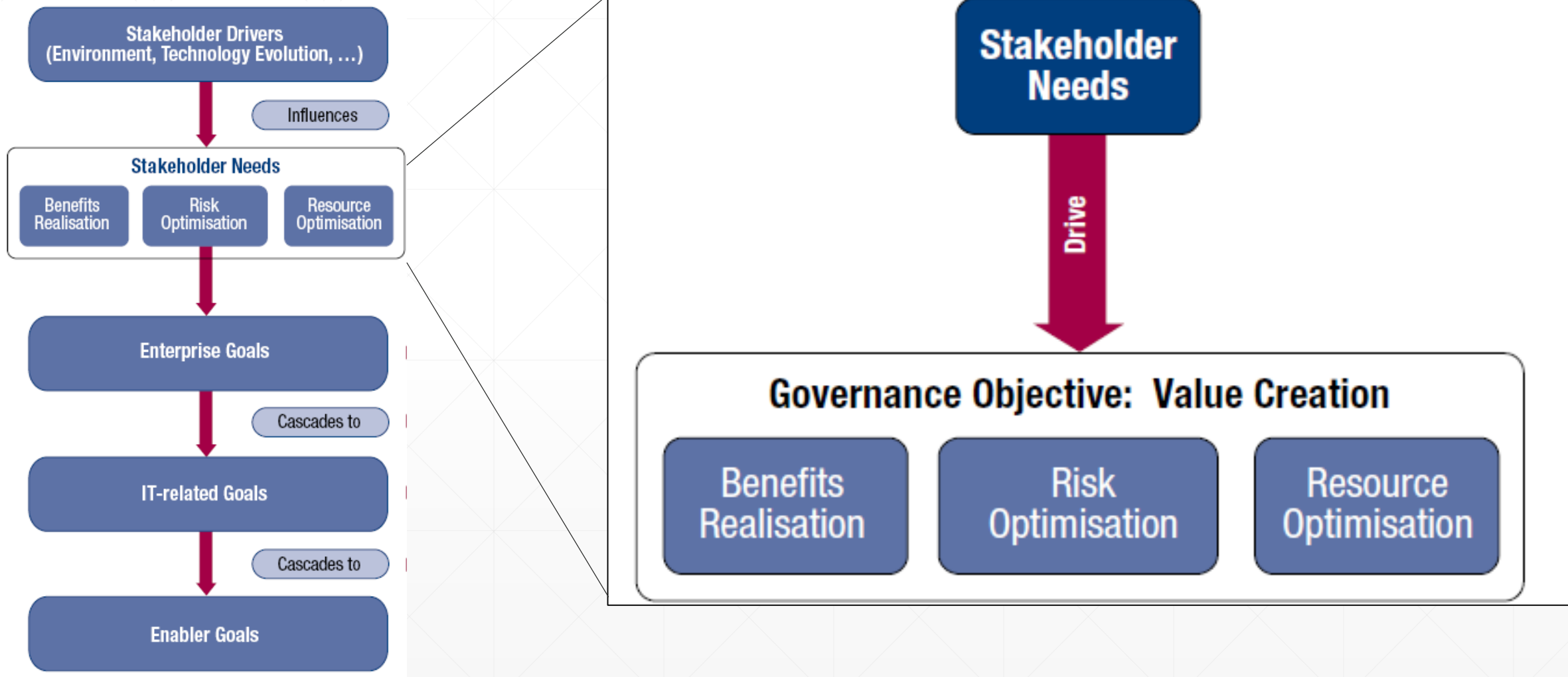


See: <https://www.nist.gov/cyberframework/informative-references>

Compliance: not the Goal but should be an Outcome



Remember?



CMMI Work on CyberMaturity

- Since 1987, CMMI has set the standard for process maturity
- In 2016, CMMI Institute became part of ISACA
- In the last year, ISACA/CMMI have developed an online subscription-based platform for organizations to perform self-assessment of a broad range of practices to:
 - Understand and record the current state
 - Determine a realistic target state based on risks and capabilities
 - Help inform senior stakeholders how the balance is going

See: <https://cmmiinstitute.com/products/cybermaturity>

Targets are Based on an Organization's Determination of its Unique Risk Profile

		Risk Events												
		RE-1c	RE-1l	RE-1a	RE-2c	RE-2l	RE-2a	RE-5	RE-7	RE-6	RE-4	RE-3c	RE-3l	RE-3a
Potential Vulnerabilities	PV-1	VH	?	VL	?	VL	VL	H	-	L	-	-	-	-
	PV-2	VH	?	VL	?	L	VL	L	-	H	-	-	-	-
	PV-3	H	?	VL	?	L	VL	H	-	L	-	-	-	-
	PV-4	VH	?	VL	?	L	VL	H	VL	H	-	-	-	-
	PV-5	L	?	VL	?	VL	VL	L	-	H	-	-	-	-
	PV-6	-	-	VL	-	-	VL	H	L	L	-	-	-	VL
	PV-7	VH	?	VL	?	L	VL	H	L	H	L	L	VL	L
	PV-8	VH	-	-	?	-	-	-	-	H	-	VL	-	-
	PV-9	VH	?	VL	?	L	VL	L	-	H	-	-	-	-
	PV-10	VH	?	VL	?	VL	VL	H	-	-	-	-	-	-
	PV-11	VH	?	VL	?	L	VL	H	-	L	-	-	-	-
	PV-12	VH	?	VL	?	VL	VL	H	VL	-	H	-	-	-
	PV-13	-	-	VL	-	-	VL	H	L	H	-	-	-	L
	PV-14	-	-	VL	-	-	VL	L	VL	-	-	-	-	-
	PV-15	-	-	VL	-	-	VL	H	-	-	-	-	-	-

For each Potential Vulnerability, users will assign the likelihood of each Risk Event resulting from Security Scenario



Once likelihood of Security Scenarios have been assigned, users will assign an impact for each Risk Event

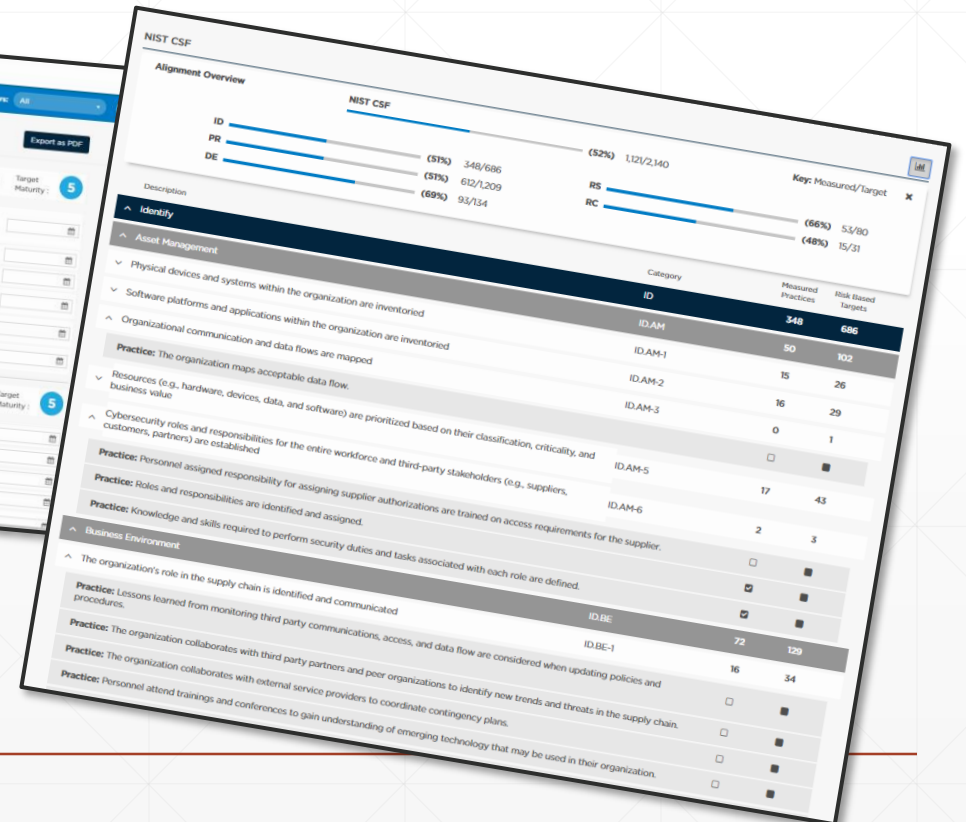
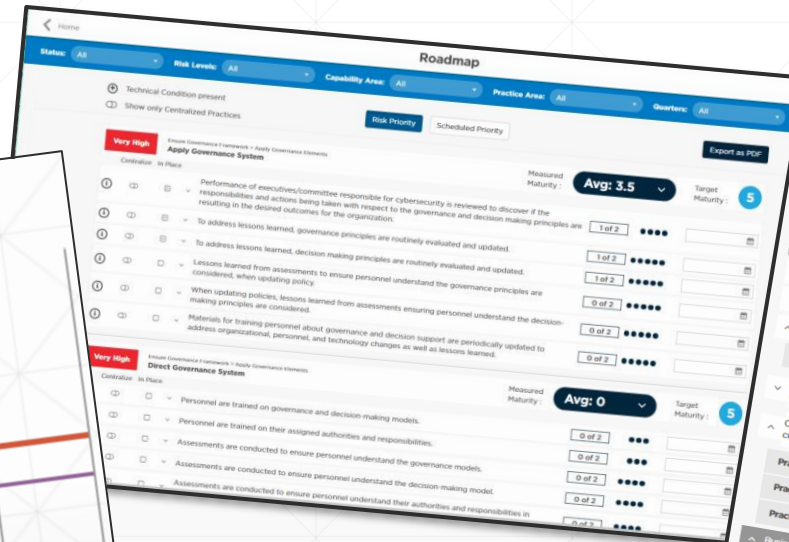
^ Hide Full Chart

CMMI-CP's Standardized Definitions of Maturity

	LEVEL 1 PERFORMED	LEVEL 2 MANAGED	LEVEL 3 DEFINED	LEVEL 4 QUANTITATIVELY MANAGED	LEVEL 5 OPTIMIZED
PEOPLE	General personnel capabilities may be performed by an individual, but are not well defined	Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization	Roles and responsibilities are identified, assigned, and trained across the organization	Achievement and performance of personnel practices are predicted, measured, and evaluated	Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external)
PROCESS	General process capabilities may be performed by an individual, but are not well defined	Adequate procedures documented within a subset of the organization	Organizational policies and procedures are defined and standardized. Policies and procedures support the organizational strategy	Policy compliance is measured and enforced Procedures are monitored for effectiveness	Policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured.
TECHNOLOGY	General technical mechanisms are in place and may be used by an individual	Technical mechanisms are formally identified and defined by a subset of the organization; technical requirements in place	Purpose and intent is defined (right technology, adequately deployed); Proper technology is implemented in each subset of the organization	Effectiveness of technical mechanisms are predicted, measured, and evaluated	Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal & external)

Self Assessment Results Produce Actionable and Meaningful Reporting

Based on assessment results we can provide Board-ready reports about as-is and to-be, alignment with standards, and a prioritized roadmap of activities to close gaps between current & target state



Take Aways

- ISACA is very pleased to join ENISA and NIST in advancing both the technical aspects of CTI and the business/governance aspects
 - Please continue to apply NIST models and guidance, and give us feedback to help us to continually improve our products
 - Please participate in ISACA requests for information and workshops so that we can continue to foster international collaboration and opportunities for sharing information
 - So many products say they're "risk-based" – please continue to work with us to define the taxonomies and metrics so that we can improve strategic planning and tactical operations
-