ENERGYSEC
SERVING THE INDUSTRY'S SECURITY COMMUNITY SINCE 2004

Framing Security-Centric Approaches to Compliance Driven Internal Controls Evaluations (ICE)

Jack Whitsitt
jack@energysec.org

Steve Parker
steve@energysec.org

Meet Your Panelists

Jack Whitsitt
Security Strategist
EnergySec

Steve Parker
President
EnergySec

It's Interactive

Please submit your questions through the control panel to get answers LIVE from our panelists.

It's Hip to Chat

EnergySec is hosting an online chat to accompany this webinar which is open to all registered EnergySec Community participants.

To join the chat as a guest, visit:

https://hipchat.energysec.org/gFxUD4pw9

If you have a HipChat account already, join us in the ICE Discussion room. Note: Registered users have access to the chat history, file attachments, and links

Webinar Goals

- Use existing frameworks to help define an ICE Framework
  - Integrate existing and future efforts
- Explore the possibility of using an ICE to bridge the gap between compliance and security
  - Controls are common elements between them
  - An ICE, although often vaguely defined and often intended primarily for compliance, can be a platform for that bridge

- Agenda:
  - What is an ICE?
  - **A Possible Approach to Creating an ICE Framework from Existing Frameworks**

NERC

NERC's ICE Direction: Unclear

This webinar is not meant to be directly in line with NERC's direction but should support it (?)

- Seems to be trying to help auditors do less
- Seems to be suggesting that having some sort of controls translation to CIP would be part of that
- Seems to be suggesting that having a control placement-to-risk alignment process could ALSO be part of that
- Seems to be suggesting that "risk" might mean either your identified business risks or compliance risks.

What is an ICE (Generally)?

- Internal Controls Evaluation:
  - A **framework** using **metrics** to **communicate** some aspects of a **controls** program against a set of **adversaries** to a set of **stakeholders**, such as **NERC**, in order to affect their behavior.

- Possibly Testing for:
  - Common **Control Suite** usage
  - Control **Program Maturity**
  - Control **Alignment** to **"Compliance & Security"** risk

What is an ICE (Generally)?

- Internal Controls Evaluation:
  - A **framework** using **metrics** to **communicate** some aspects of a **controls** program against a set of **adversaries** to a set of **stakeholders**, such as **NERC**, in order to affect their **behavior**.

- Possibly Testing for:
  - Common **Control Suite** usage
  - Control **Program Maturity**
  - Control **Alignment** to **"Compliance & Security"** risk

Frameworks?

- Frameworks are a set of assumptions, concepts, values, and practices that constitutes a way of viewing reality.
  - "In Software, a framework is often a layered structure indicating what kind of programs can or should be built and how they would interrelate."
- Frameworks are composed of:
  - A structure
  - The content that structure contains or refers to
- The purpose of Frameworks is to, through structure, influence or direct human behavior.
- This is a form of communication

An ICE Framework can guide program implementation, design, execution, or use

Communication?

- **The imparting or exchanging** of information or news.
- The **successful** conveying or sharing of ideas and feelings.
- The discipline of communication focuses on how people use **messages** to generate meanings within and **across various contexts, cultures, channels, and media**.
- **Two-way process** of **reaching mutual understanding**, in which participants not only exchange (encode-decode) information, news, ideas and feelings but also **create and share meaning**. In general, communication is a means of **connecting people or places**.

An ICE Framework is too complicated or detailed, is it effective at communicating in a way that creates intended behavior?

Controls?

- What do controls do?
  - Prevent
  - Detect
  - Correct
- Two levels of control:
  - Control for Value
  - Control the Control
- Need Context for Definition and Implementation:
  - Goals
  - Metrics
  - Stakeholders & their Levers

This is critical for an ICE:

Without context, controls are just practices

Metrics?

- Metrics provide indicators to a set of stakeholders that help them decide what behaviors they need to change to achieve a state of the world that serves their purposes
  - **Who:** Who is receiving the metric? What are they trying to achieve? Who does the metric come from? Does the metric need to go elsewhere?
  - **What:** Which questions are being posed and answered?
  - **How**: What levers or processes are available to be used to affect change by which stakeholders?

Contrast this with the idea of "measurement": The documentation of a value or state without any associated action or meaning

Meaningful ICE metrics require some focusing on desired outcomes and internal environment, possibly beyond the direct applicability of the controls being evaluated.

Stakeholders & Behavior?

When we are talking “Controls Evaluation” – or anything else - who we are communicating with matters to how we shape the message

Grudge Holders	Motivations, Goals, Resources, Partners, Enemies
Fire Setters	Vulnerabilities, Tools, Infrastructure, Tactics, Employer
Fire Fighters	Vulnerabilities, Tools, Infrastructure, Tactics, Employer
Fire Code Writers	Controls, Risks, Standards, Metrics, Maturity, Process
Fire Code Inspectors	Auditing, Controls, Metrics, Compliance
Victims	Privacy, Consequence, Compensation, Protection, Law, Emotion
Asset Owners	Risk, Likelihood, Compliance, Reputation, Cost
Equipment Vendors	Features, Controls, Reliability, Solutions
Government	Partnership, Assurance, Protection, Regulation
Reporters	Are they going to shut down the power grid like in that movie?

Control Suites?

- MANY Information Security Control Frameworks Exist
  - SANS, NISTCSF, Etc.
- Discuss types of controls but rarely provide implementation specifics
  - Specificity requires context
  - Context is defined by business environment and exposure
  - These also define how businesses make money
  - Obvious conflict of interest in scope

Program Maturity?

- Program maturity can be described with implementation metrics with descriptions such as
  - Fully implemented
  - Partially implemented
- Program maturity may also be described with quality metrics with descriptions such as
  - Partially Repeatable
  - Reliably Executed
- This is what the C2M2 attempts to accomplish for information security programs

The same concepts can also be applied to an ICE: What questions is the ICE answering?

Alignment?

- Controls should Achieve Business Value
  - What is it? How is it measured?
  - Compliance, Reputation, Availability, etc.
- Value is determined by the intersection of Adversaries and Stakeholders
  - Enable
  - Prevent
- Being able to adjust is critical
  - Adversaries are thoughtful
  - Stakeholder needs evolve
- This is helped by having a repeatable, relatable framework
  - Both Concepts & Process

Your processes may vary, but a good ICE framework should related concepts in a way that allows different processes to be clearly applied to the same problem.

Cybersecurity?

- **Secure system:** One that does no more or less than we want it to for the amount of effort and resources we're willing to invest in it.

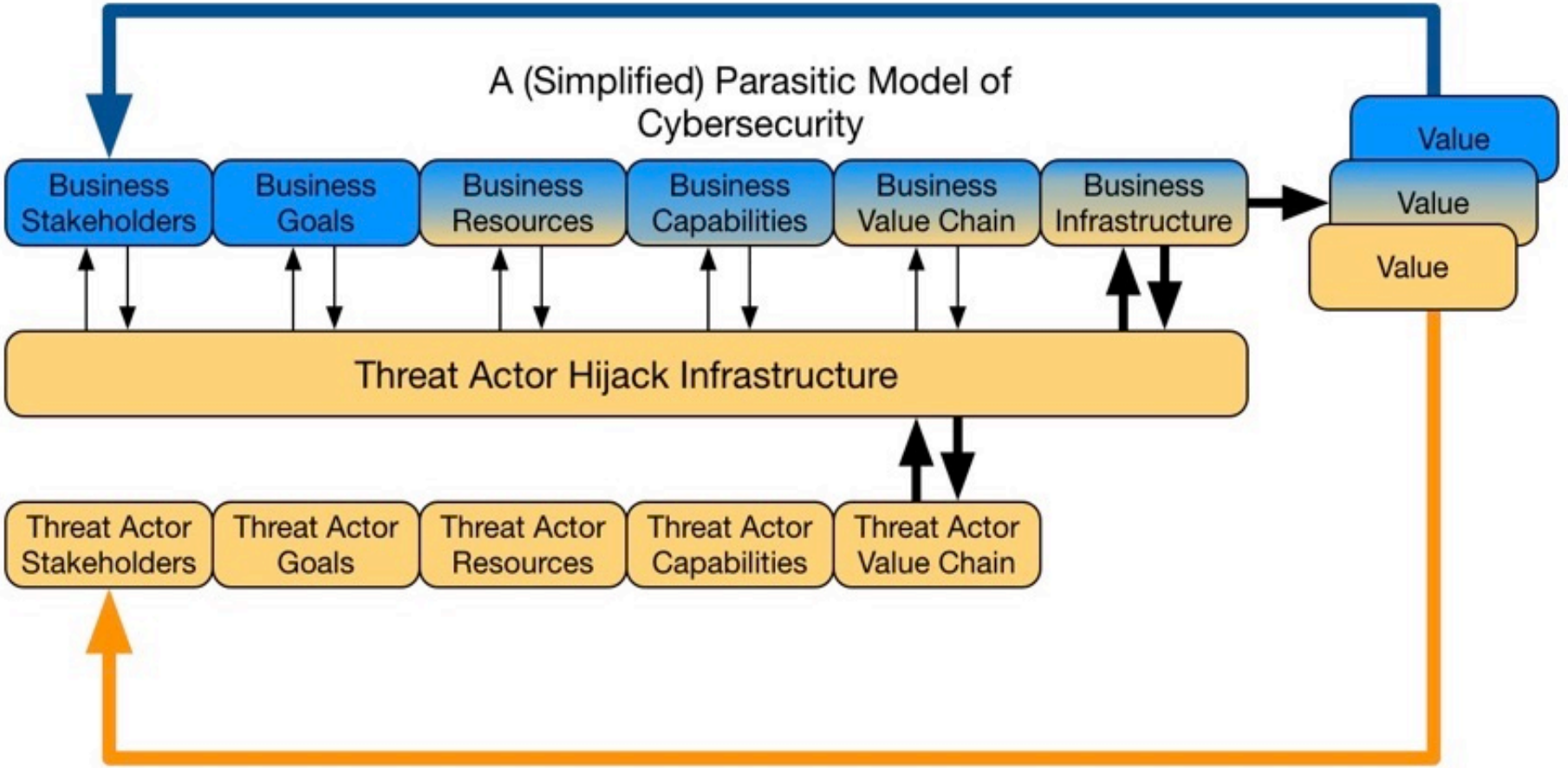
- **Cybersecurity:** The enablement of an environment in which business objectives are sustainably achievable by Information Security, Control Systems Security, and Other Related Security Activities in the face of continuous risk resulting from the use of cyber systems.

- **Cyber Risk:** the possibility that actors will use our systems as a means of repurposing our value chains to alter the value produced, inhibit the value produced, or produce new value in support of their own value chains.

An ICE, even in support of compliance, should always provide positive value to the environment in which Information Security programs are executed in a way that helps secure systems and reduced risk.

Even if this means treating auditors as adversaries?

Adversaries?



(Control Based) Compliance?

- Control Compliance:
  - The verification of controls and their placement with the **intent of deriving some knowledge about (or assuring) the security state of a system** through a series of positive and negative incentives.
  - Attempts to **aid implementation** of security by **constraining decision making options as they pertain to controls**

- Has (at least) two problems:
  - Simply constraining decision making outcomes risks creating **a locked-in "foosball team" to play against a real life "soccer team"**
  - Whether controls are effective at **reducing security risk depends on many factors not measured by control compliance** and assumes environmental variables which may not be true

An ICE *can* provide some of the flexibility needed to mitigate the former and *can* provide a place for communicating information to mitigate the latter.

Recall: NERC

- Seems to be trying to help auditors do less
- Seems to be suggesting that having some sort of controls translation to CIP would be part of that
- Seems to be suggesting that having a control placement-to-risk alignment process could ALSO be part of that
- Seems to be suggesting that "risk" might mean either your identified business risks or compliance risks.

Left up to us to link Audit Risk ICE to Security Risk ICE; if we choose to do so at all or if it's even possible

ENERGYSEC
SERVING THE INDUSTRY'S SECURITY COMMUNITY SINCE 2004

An Approach to Creating an ICE Framework

Approach

- Control Suite:
  - Use NISTCSF to provide control depth and interoperability to ICE
- Program & Control Maturity:
  - Use C2M2 Structure for measurement/metrics
- Compliance:
  - Swap out C2M2 Domains for CIP Requirements
- Security:
  - Mappings to Risk Management/Security Frameworks

NISTCSF

- Government led, industry developed
- Primarily consists of generic practice statements
- Goal is standardization and integration of language and practices across Stakeholders, not implementation standards
- Does not provide “How” guidance, context, metrics, or process
- No risk or compliance alignment mechanisms
- Limited utility in existing structure
- http://www.nist.gov/cyberframework/

NISTCSF

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NISTCSF

Function	Category	Subcategory	Informative References
			SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI - 4
		DE.AE-5: Incident alert thresholds are established	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is	• **ISA 62443-2-1:2009** 4.3.3.3.8

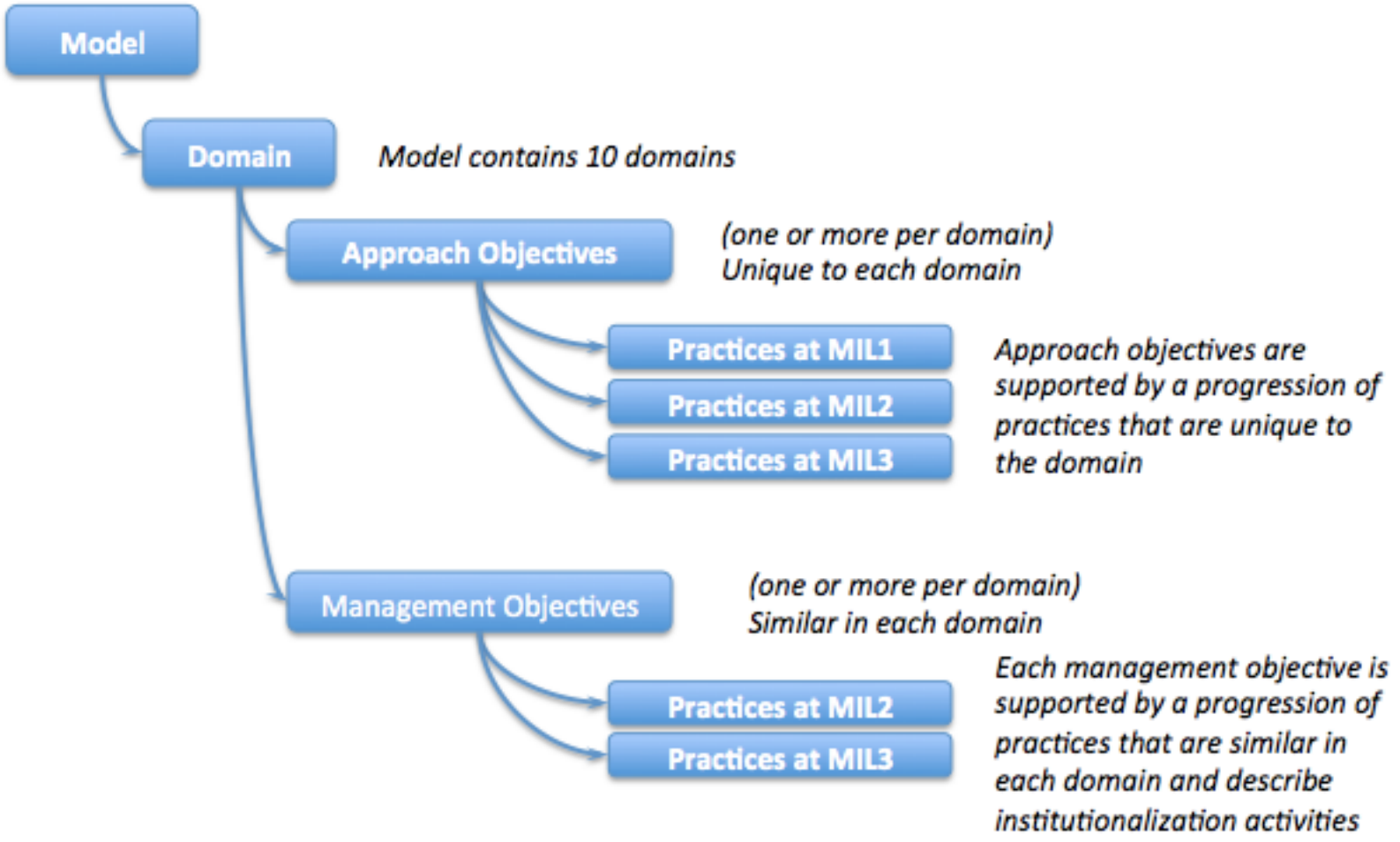
C2M2

- DOE developed, widely accepted
- Focus on Measures and Metrics through Structure
- Increasingly advanced practice sets associated with each "Approach" MIL
  - Indicates "Completeness"
- Increasingly advanced Organizational Management behaviors associated with each "Management" MIL
  - Indicates "Quality" for each level of "Completeness"
- Controls differ by Domain, Management Behaviors do not
- Still does not tell you how to align with risks, adversaries, or stakeholders
- http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity

C2M2

DOMAIN	DOMAIN DESCRIPTION
Risk Management (RM)	Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.
Asset, Change, and Configuration Management (ACM)	Manage the organization's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.
Identity and Access Management (IAM)	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.
Threat and Vulnerability Management (TVM)	Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.
Situational Awareness (SA)	Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP).
Information Sharing and Communications (ISC)	Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.
Event and Incident Response, Continuity of Operations (IR)	Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.
Supply Chain and External Dependencies Management (EDM)	Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.
Workforce Management (WM)	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.
Cybersecurity Program Management (CPM)	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

C2M2: Two Scores



C2M2:
"Risk Management" Domain Example

	Manage Cybersecurity Risk	Management Practices
MIL1	a. Cybersecurity risks are identified b. Identified risks are mitigated, accepted, tolerated, or transferred	1. Initial practices are performed but may be ad hoc
MIL2	c. Risk assessments are performed to identify risks in accordance with the risk management strategy d. Identified risks are documented e. Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy f. Identified risks are monitored in accordance with the risk management strategy g. A network (IT and/or OT) architecture is used to support risk analysis	1. Practices are documented 2. Stakeholders of the practice are identified and involved 3. Adequate resources are provided to support the process (people, funding, and tools) 4. Standards and/or guidelines have been identified to guide the implementation of the practices
MIL3	h. The risk management program defines and operates risk management policies and procedures that implement the risk management strategy i. A current cybersecurity architecture is used to support risk analysis j. A risk register (a structured repository of identified risks) is used to support risk management	1. Activities are guided by policies (or other organizational directives) and governance 2. Activities are periodically reviewed to ensure they conform to policy 3. Responsibility and authority for performing the practice is clearly assigned to personnel 4. Personnel performing the practice have adequate skills and knowledge

C2M2 & NIST

- C2M2 Provides an Advanced Structure for identifying completeness and quality of Information Security approaches without alignment to risk or compliance
  - Controls are difficult to extract from the framework for their own use
- NISTCSF Provides a Consensus list of Common Information Security practices without providing completeness or quality measures and without aligning to risk or compliance
  - Practices are easily extractable from structure and can be used to develop controls
- Using the structure of C2M2 with the Standards of CIP and the Practices of NISTCSF, an ICE Framework can be created which evaluates Controls in terms of
  - Security alignment
  - Compliance alignment
  - Quality of programs (as applied to controls)
  - Other consensus control sets

NERC CIP

(CIP) Critical Infrastructure Protection (82)

Subject to Future Enforcement (12)

CIP-002-5.1	Cyber Security — BES Cyber System Categorization
CIP-003-5	Cyber Security - Security Management Controls
CIP-004-5.1	Cyber Security — Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-5	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-5	Cyber Security - System Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-5	Cyber Security - Recovery Plans for BES Cyber Systems
CIP-010-1	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-1	Cyber Security - Information Protection
CIP-014-1	Physical Security
CIP-014-2	Physical Security

Putting it Together: Developing an ICE Framework Step 1

Substitute CIP Standards for C2M2 Domains

(CIP) Critical Infrastructure Protection (82)

Subject to Future Enforcement (12)

CIP-002-5.1	Cyber Security — BES Cyber System Categorization
CIP-003-5	Cyber Security - Security Management Controls
CIP-004-5.1	Cyber Security — Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-5	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-5	Cyber Security - System Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-5	Cyber Security - Recovery Plans for BES Cyber Systems
CIP-010-1	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-1	Cyber Security - Information Protection
CIP-014-1	Physical Security
CIP-014-2	Physical Security

DOMAIN
Risk Management (RM)
Asset, Change, and Configuration Management (ACM)
Identity and Access Management (IAM)
Threat and Vulnerability Management (TVM)
Situational Awareness (SA)
Information Sharing and Communications (ISC)
Event and Incident Response, Continuity of Operations (IR)
Supply Chain and External Dependencies Management (EDM)
Workforce Management (WM)
Cybersecurity Program Management (CPM)

Putting it Together: Developing an ICE Framework Step 2

- Map NISTCSF Practices to CIP Standards

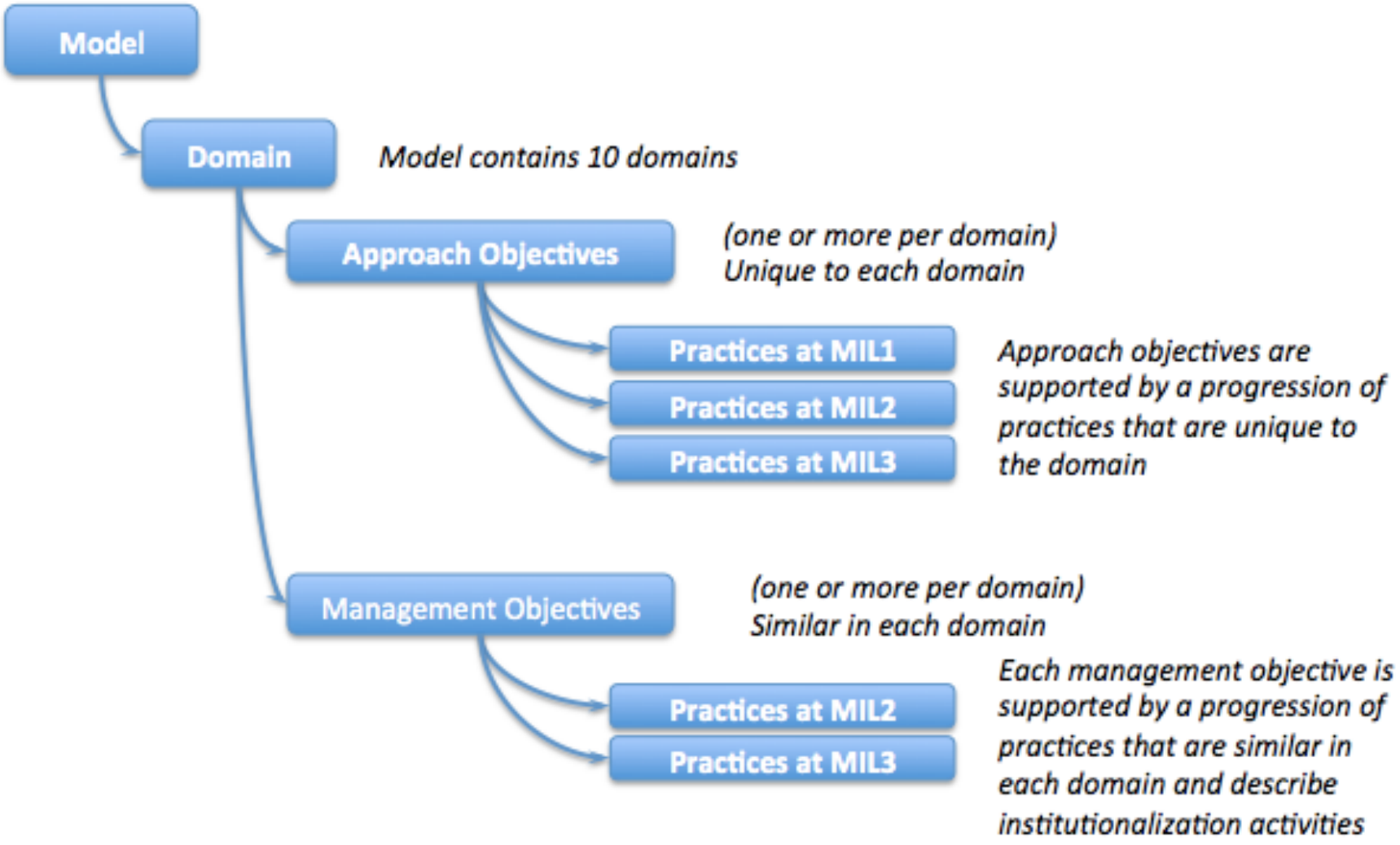
NERC CIP STANDARD		NISTCSF Practices
2	5.1 R1	ACM-1a
		ACM-1b
		EDM-1a
		RND-1a
		ACM-1c
		ACM-1d
		EDM-1c
		RND-1b
		RM-1c
		ACM-1e
		TVM-1i
		RND-1c

Putting it Together: Developing an ICE Framework Step 3

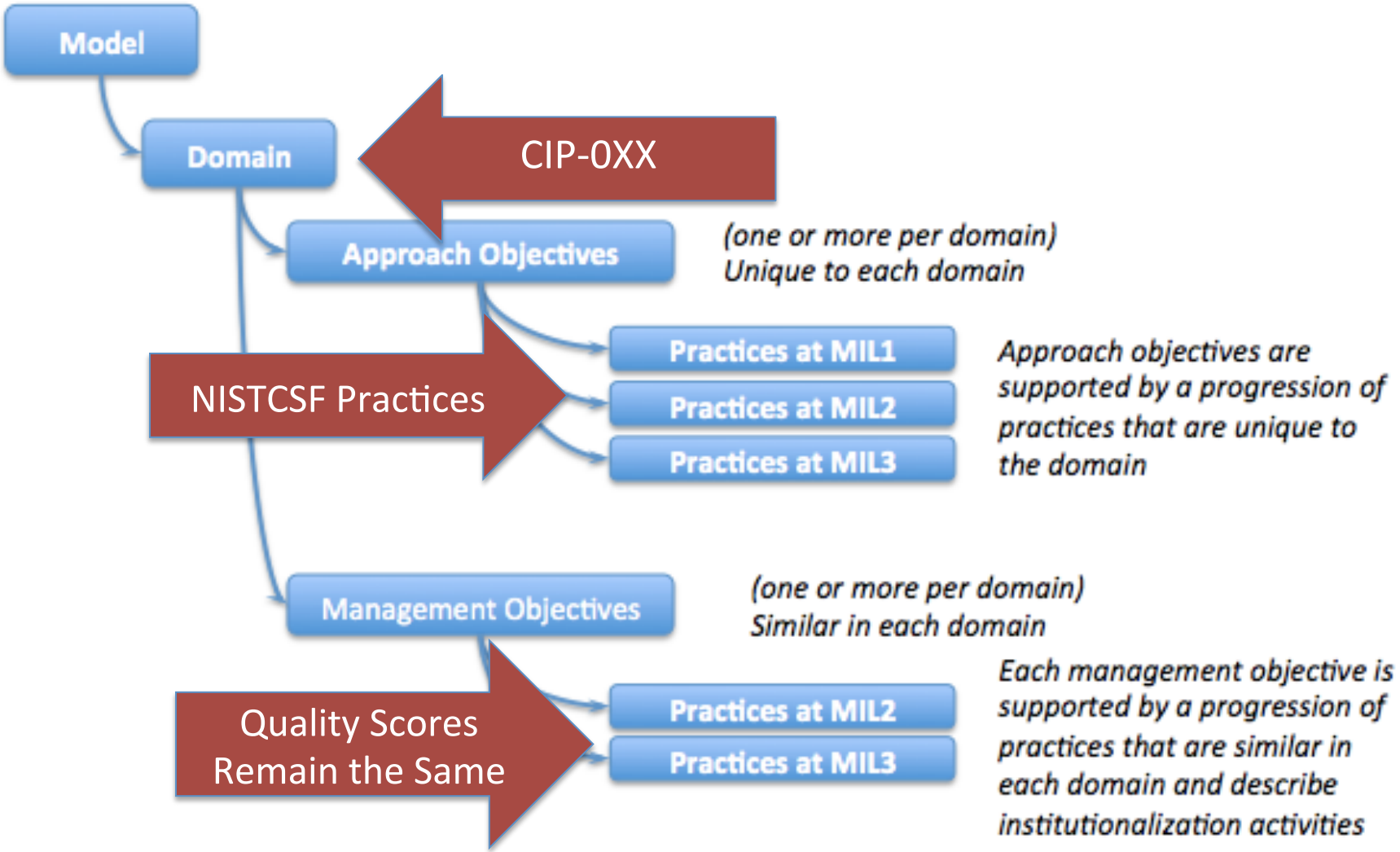
- Organize NISTCSF Practices into MIL's on a per-CIP Standard Basis.
- Add a quality Score (1-3) per MIL

NERC CIP STANDARD		NISTCSF Practices		
		MIL 1	MIL 2	MIL 3
2	5.1 R1	ACM-1a	ACM-1c	RM-1c
		ACM-1b	ACM-1d	ACM-1e
		EDM-1a	EDM-1c	TVM-1i
		RND-1a	RND-1b	RND-1c
		QUALITY SCORE	QUALITY SCORE	QUALITY SCORE

Recall: C2M2 Structure



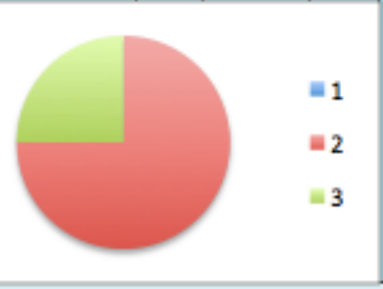
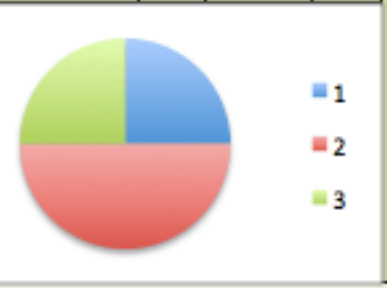
Now: C2M2 Structure with CIP/NIST



Putting it Together: Developing an ICE Framework Step 4

- Score Each CIP Standard

CIP-002: MATURITY AND QUALITY SCORES IN TERMS OF NISTCSF CONTROL IMPLEMENTATION

	MIL 1					MIL 2					MIL 3				
	NISTCSF	Full	Partial	Not	Qual MIL	NISTCSF	Full	Partial	Not	Qual MIL	NISTCSF	Full	Partial	Not	Qual MIL
5.1 R1	ACM-1a ACM-1b EDM-1a RND-1a	2	1	1	3	ACM-1c ACM-1d EDM-1c RND-1b	0	3	1	1	RM-1c ACM-1e TVM-1i RND-1c	1	2	1	1
	MIL 1 TOTAL	PERCENTAGE			QUALITY	MIL 2 TOTAL	PERCENTAGE			QUALITY	MIL 3 TOTAL	PERCENTAGE			QUALITY
	4	50	25	25	2.5	4	0	75	25	1	4	25	50	25	1.5
															
	MIL 1 SCORES					MIL 2 SCORES					MIL 3 SCORES				

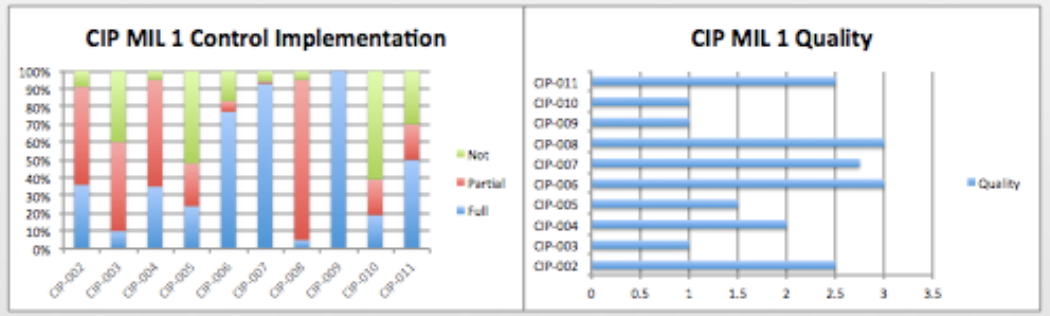
Putting it Together: Developing an ICE Framework Step 5

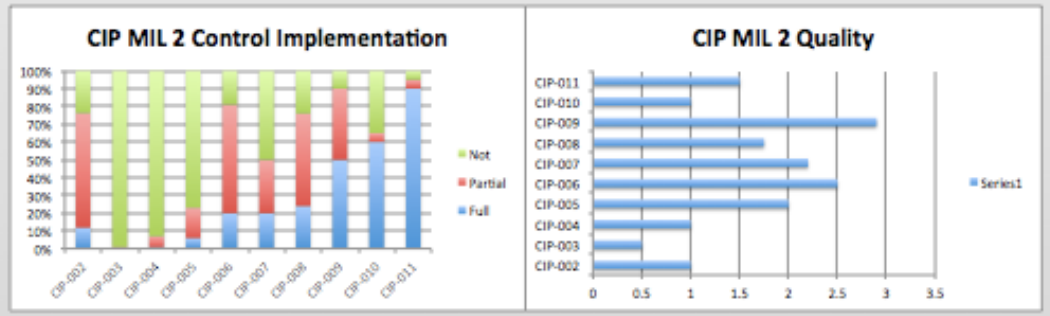
- Control Status Evaluation
  - How many are implemented
  - At what level of maturity
  - At what level of quality

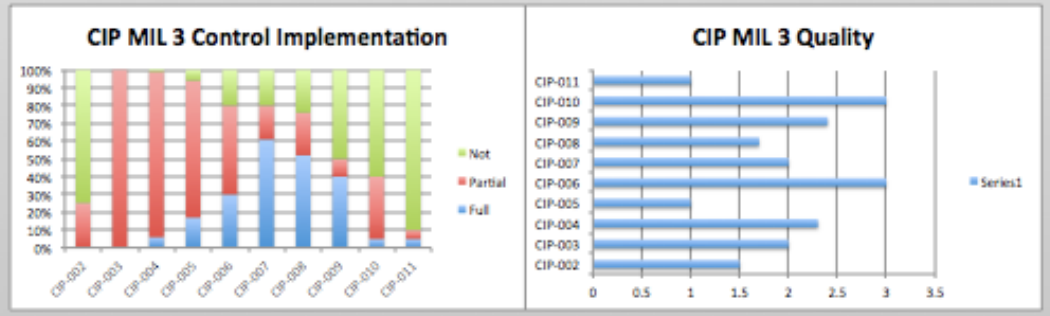
Still does not answer:

What does control implementation look like specifically?

This requires security context because NISTCSF is too generic.







Putting it Together: Developing an ICE Framework Step 6

Develop Security Context for Control Specificity by:

- Identifying Business Risks/Goals to be Managed by Security Controls
- Develop Business & Technical Requirements for NIST Practices to Define Implementation Needs based on these business Risks/Goals
- These requirements turn NIST Practices into Controls which can be Measured in an ICE Context: Implementation Completeness and Quality

	BUSINESS GOAL FOR SECURITY	
	BUSINESS CONTROL REQUIREMENTS	TECHNICAL CONTRL REQUIREMENTS
NIST FRAMEWORK CONTROLS		

NIST FRAMEWORK CONTROLS		BUSINESS GOAL FOR SECURITY: Assure Reputation by minimizing likelyhood of Executives Creating Security Exposure | Sub Goal: Minimize effectiveness of targeting Phishing Campains													
		Scale/Quality	Strategy	Resources	Constraints	Capabilities	Value Chain	Users	Applications	Data	OS	Network	Physical	Lifecycle	Security
Awareness Training	PR.AT-4; Senior executives understand roles & responsibilities	Training must account for a wide range of types of phishing and executive behavior that can lead to phishing; training cannot be done to a list; all executives must be reminded over time	Executive Traning Plan will need an executive sponsor			HR and IT and Security must work together to develop targeted Executive Training Plan	Training must occur when a new executive is hired as part of the onboarding value chain element and during any HR maintenance activities	Training and Testing must affect specific user (executive behavior). What is that behavior?	Applications should be chosen and configured in a way that is easy to educate and train on						
Continuous Monitoring	DE.CM-1; The network is monitored to detect potential cybersecurity events	A lot of normal email looks like phishing and vice versa. At high volume, this cannot be done manually	IT email systems must allow Security monitoring solutions	Budget must be included for phishing monitoring		All capabilities must work with Security to provide information about their use cases to enable better monitoring	Security must be aware of value chain details t o sort good/bad emails	Users should report phishing attempts to Security to enhance detection	Applications should, where possible, log details for Security monitoring						Information about existing phishing campaigns should be pulled in from external sources

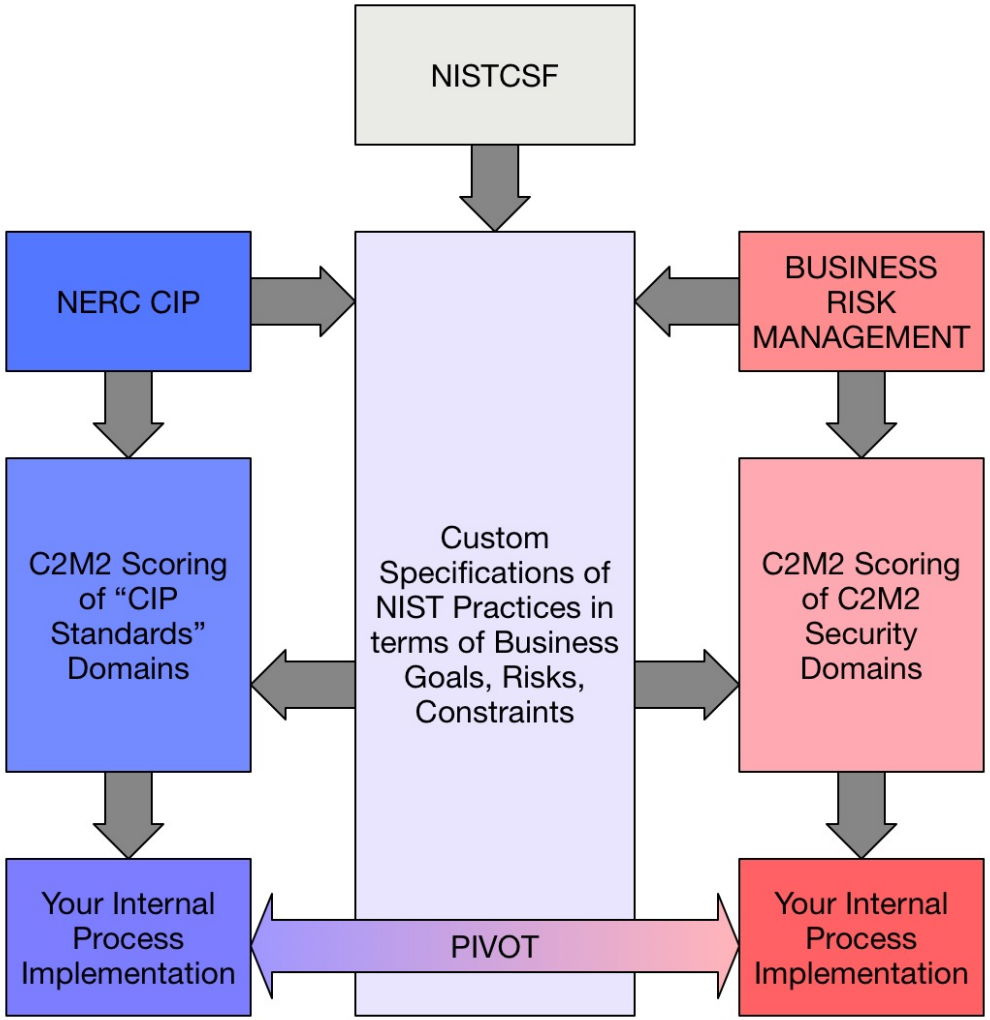
Putting it Together: Developing an ICE Framework Step 6

This should be populated by your business risk management process.

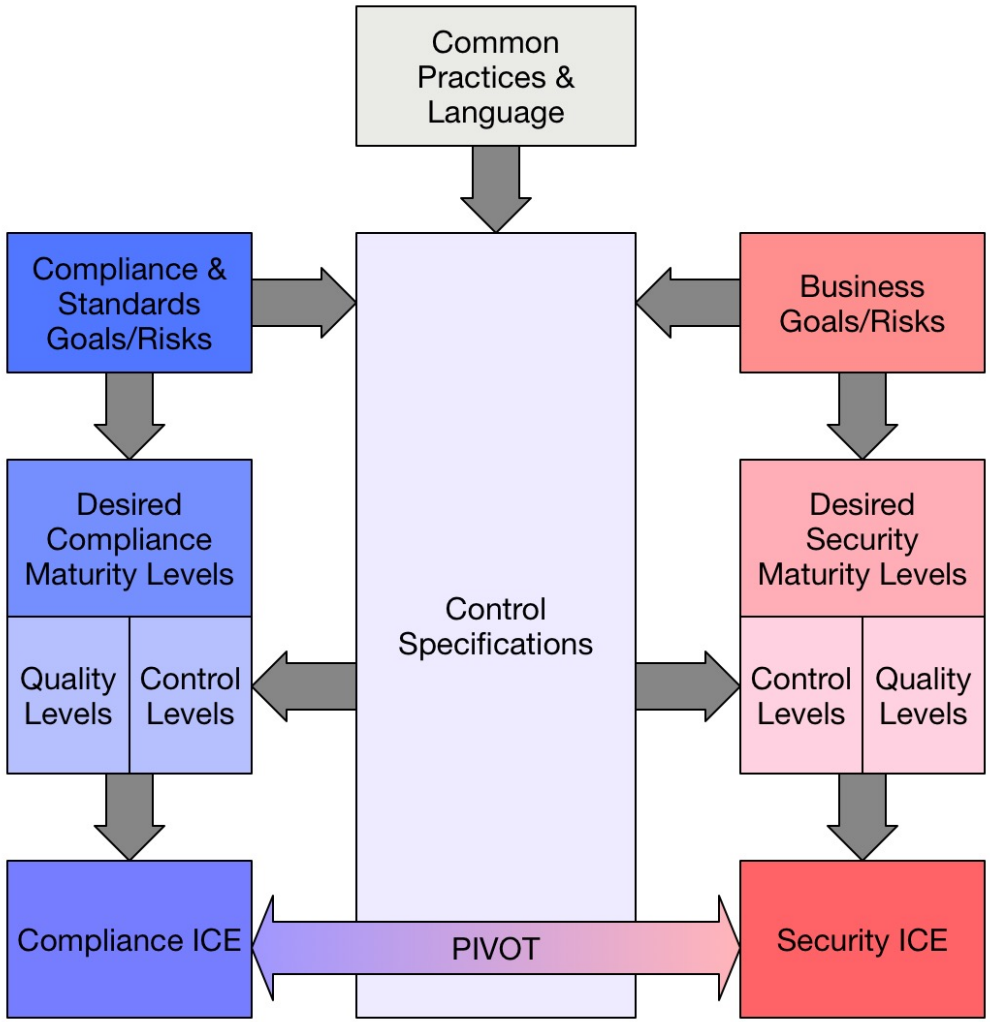
	BUSINESS GOAL FOR SECURITY	
	BUSINESS CONTROL REQUIREMENTS	TECHNICAL CONTRL REQUIREMENTS
NIST FRAMEWORK CONTROLS		

NIST FRAMEWORK CONTROLS		BUSINESS GOAL FOR SECURITY: Assure Reputation by minimizing likelyhood of Executives Creating Security Exposure | Sub Goal: Minimize effectiveness of targeting Phishing Campains													
		Scale/Quality	Strategy	Resources	Constraints	Capabilities	Value Chain	Users	Applications	Data	OS	Network	Physical	Lifecycle	Security
Awareness Training	PR.AT-4; Senior executives understand roles & responsibilities	Training must account for a wide range of types of phishing and executive behavior that can lead to phishing; training cannot be done to a list; all executives must be reminded over time	Executive Traning Plan will need an executive sponsor			HR and IT and Security must work together to develop targeted Executive Training Plan	Training must occur when a new executive is hired as part of the onboarding value chain element and during any HR maintenance activities	Training and Testing must affect specific user (executive behavior). What is that behavior?	Applications should be chosen and configured in a way that is easy to educate and train on						
Continuous Monitoring	DE.CM-1; The network is monitored to detect potential cybersecurity events	A lot of normal email looks like phishing and vice versa. At high volume, this cannot be done manually	IT email systems must allow Security monitoring solutions	Budget must be included for phishing monitoring		All capabilities must work with Security to provide information about their use cases to enable better monitoring	Security must be aware of value chain details t o sort good/bad emails	Users should report phishing attempts to Security to enhance detection	Applications should, where possible, log details for Security monitoring						Information about existing phishing campaigns should be pulled in from external sources

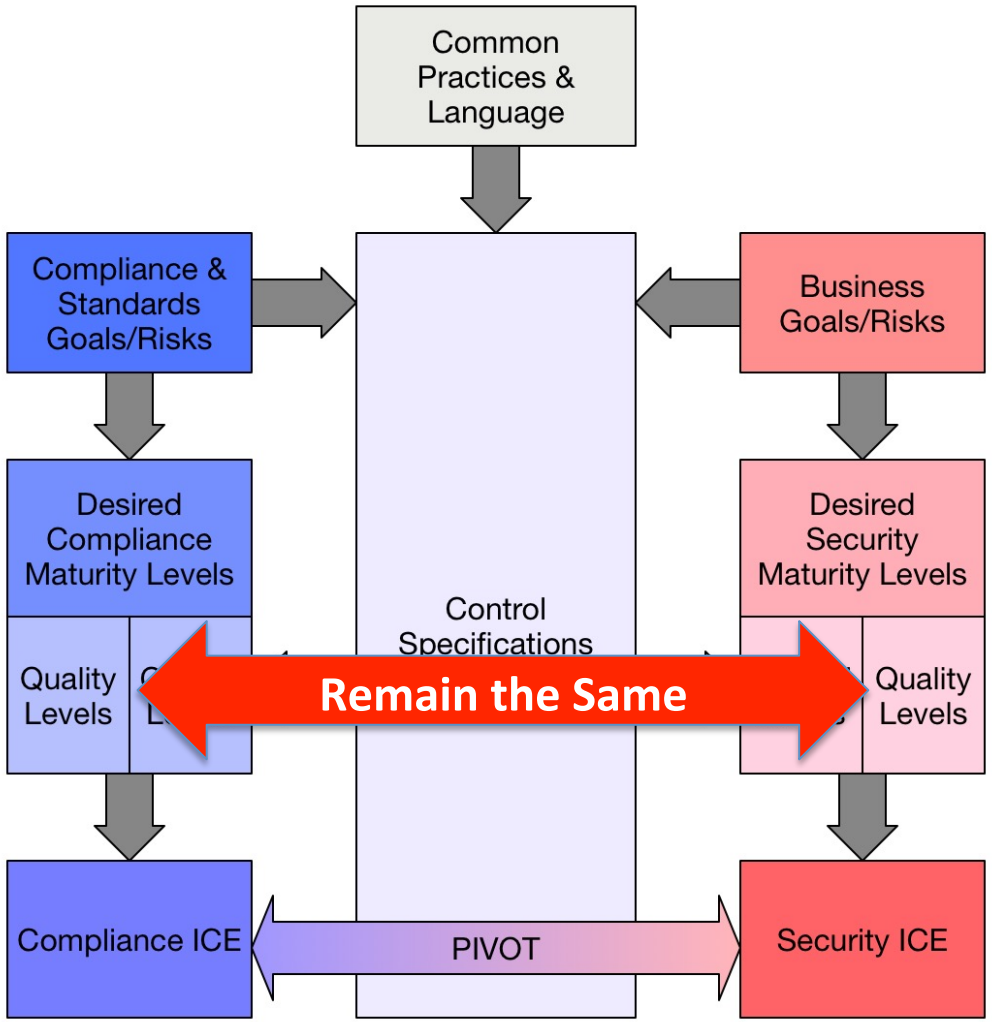
Putting it Together: High Level



Putting it Together: High Level



Putting it Together: High Level



Putting it Together: Benefits of Combining NISTCSF/C2M2/CIP

- By using NIST Practices as a common language:
  - Multiple measures for multiple stakeholders against multiple adversaries (including auditors) can be created and linked
- By using a C2M2-like scoring structure:
  - Evaluations of Controls against Standards Compliance and Security Risk Reduction can be compared.
- Business Risks and Goals used to contextualize NIST practices into measurable controls for compliance purposes can also be:
  - Used for prioritizing C2M2 Domain Maturity goals for risk reduction

What's the real value?

- What value beyond compliance should an ICE provide? Can it provide?
  - Common **control suites** usage: NISTCSF
  - Control **program maturity:** Practice Level & Quality
  - Control alignment to **"security"** risk: C2M2 Domains
  - Control alignment to "**compliance**" risk: CIP in C2M2
  - Alignment Pivoting: Common Controls & Metrics
- What value WILL and ICE provide?
  - It depends on your adversary, stakeholder, and risk contexts

Closing

- This approach requires finding or making your own Mappings
  - How you map is less important than having one
- Other guidance may differ and other approaches are valid
  - Fundamentals should be similar
- Learn more about evaluating, creating, combining, and using security frameworks to effectively reduce risk in a two-day class:
  - **http://www.energysec.org/upcoming-live-events/**

Questions

Thank You

EnergySec
The National Energy Sector Cyber Security Organization

Jack Whitsitt
Security Strategist
jack@energysec.org

Steve Parker
President
steve@energysec.org