

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



Determining Current Cybersecurity Capabilities

Develop and maintain an unrivaled, globally competitive cybersecurity workforce

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



NICE Cyber Workforce Inventory Project

Dr. Michael Koehler

Program Analyst

U.S. Department of Homeland Security

NICE Cyber Workforce Inventory Project

Understanding the State of the Cyber Workforce

- Lead – U.S. Department of Homeland Security

Background

National Initiative for Cybersecurity Education (NICE)

- **Goal 2:** Broaden the pool of skilled workers capable of supporting a cyber-secure nation.
- **Goal 3:** Develop and maintain an unrivaled, globally competitive cybersecurity workforce

Mission

Strengthen the overall cybersecurity posture of the United States by collecting data that captures current cyber workforce capabilities and analyzing that data to identify the current state of the workforce.

Vision

Inform the development and enhancement of cybersecurity education to foster a cybersecurity workforce capable of defending the infrastructure and interests of the United States.

Foundation

The NICE Cybersecurity Workforce Framework

- 7 Categories
- 31 Specialty Areas
- Numerous Associated Tasks and KSA

Presentations

To provide an overview of the methods, challenges, and best practices for investigating cybersecurity workforce capabilities and competencies.

Presenters

Maureen Higgins/Dr. Jacqueline Caldwell, OPM

- Federal Cybersecurity Competency Model

Drew Lopez, Booz Allen Hamilton

- DHS Cyber Workforce Initiative

Dr. David Tobey, NBISE

- From Cybersecurity Competencies to a Job Performance Model

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



Federal Cybersecurity Competency Model

Maureen Higgins/Dr. Jacqueline Caldwell

Assistant Director, Agency Support & Technical Assistance/Personnel Research Psychologist

U.S. Office of Personnel Management

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



DHS Cyber Workforce Initiative

Drew Lopez, SPHR, MHCS

Lead Associate - Human Capital and Learning Team

Booz Allen Hamilton

DHS Cyber Workforce Initiative

The Secretary of the Department of Homeland Security has identified the acquiring, growing, and sustaining of a cyber workforce as one of the Department's priorities


- The cyber security mission of DHS will require a federal workforce that possesses the necessary skills to lead cybersecurity missions and solutions, while ensuring the future security of the national critical infrastructure
- In response, the Office of the Chief Human Capital Officer (OCHCO) and the National Protection and Programs Directorate (NPPD) has established a cross-component team responsible for the development of this initiative

Secretary
U.S. Department of Homeland Security
Washington, DC 20528



Homeland
Security

December 21, 2010

MEMORANDUM FOR: Component Heads
FROM: Secretary Napolitano 
SUBJECT: The U.S. Department of Homeland Security Workforce Strategy for FY 2011-2016

I am pleased to share the *U.S. Department of Homeland Security (DHS) Workforce Strategy for FY 2011-2016*, developed collaboratively to enrich and strengthen the entire DHS community. Much progress is being made across the Department with regard to the recruitment, hiring, and development of a top-notch workforce, yet there is much work still to be done.

The *DHS Workforce Strategy* appropriately takes a broad and long-term view. Nonetheless, I expect to see immediate impacts in a variety of areas within the first 90 days, six months, and year of implementation, including:

Developing a DHS-wide leader development framework. An integrated, Department-wide framework for leader development will provide a cadre of leaders able to maximize the Department's performance and strengthen a culture of joint operations and planning. A seamless continuum of leader development that cuts across levels will enhance employee engagement, development, and retention, and hence the Department's mission effectiveness. I have asked Deputy Secretary Lute to work closely with Chief Human Capital Officer Jeffrey Neal to ensure this framework is developed and implemented expeditiously. *With cross-Department planning underway, I will look for a strategic framework to be in place by January 31, 2010, with specific training to be completed by September 30, 2011.*

Implementing a Balanced Workforce Strategy. Ensuring a balanced workforce where governmental functions are performed by federal employees while appropriate functions are undertaken by contractors will ensure full governmental control of mission, enhance institutional knowledge, and potentially generate cost efficiencies. The use of a consistent Balanced Workforce Strategy across DHS will result in an appropriate balance of federal employees and contractors and aid in the identification of crucial workforce skills needs. *I expect the Balanced Workforce Executive Steering Group to have completed initial balanced workforce plans based on results of the Balanced Workforce Strategy by January 31, 2010, and then to add balanced workforce plans each quarter of FY 2011, after examining work that has been prioritized for review.*

Establishing a cybersecurity workforce recruitment and development strategy. The increasingly sophisticated and pervasive nature of cyber threats to our national security demands

www.dhs.gov

Implementation: First Steps

To start, Cyber Workforce Development is focused on defining *Capability* needs, which is accomplished by building competency models

- Why Cyber Competency Models?
 - Objective: Competencies define the skills/capabilities critical for successful job performance across Cyber roles, and the behaviors that exemplify the progressive levels of proficiency associated with these competencies
 - Impact: Provides a solid foundation upon which targeted recruitment, selection, and employee development (learning and training) initiatives can be built to increase Cyber Workforce capabilities

What makes a Competency Model?

- Competencies
- Behavioral Indicators

Customer Service and Technical Support: Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).		
Behavioral Indicator (BI)		
Basic (BI)	Intermediate (BI)	Advanced (BI)
<ul style="list-style-type: none"> ➤ Configures change requests with guidance by reviewing request, determining whether request is valid/reasonable, communicating with user—if necessary, and by making the appropriate change in the system 	<ul style="list-style-type: none"> ➤ Provides guidance on configuring change requests by creating training and written documents (e.g., manuals) in a clear format for staff on how to complete change requests 	<ul style="list-style-type: none"> ➤ Conducts brown bag sessions (term used for internal training), training users on how to use various tools and products (how to run queries, generate reports) ➤ Provides approval/disapproval on role-based access/content/active channel requests by reviewing whether requests comply with organizational standards and procedures ➤ Delegates change actions to the systems engineers by creating clear instructions on how to

Example

Competency	Definition
Penetration Testing	Designs, simulates, and executes attacks on networks and systems. Leverages existing and emerging methods to attack systems and exploit vulnerabilities. Documents penetration testing methodology, findings, and resulting business impact.

Implementation: Challenges

- How do we minimize the time impact on the managers, supervisors and SMEs?
- How do we ensure consistency in terminology across all agencies and components?
- Who are the DHS Cybersecurity professionals?
- What competency work has been accomplished?
- With so many Occupational Series involved with Cybersecurity, how should the models be built?

A NICE Solution

Although we still have some outstanding challenges, the NICE Framework presented an exceptional solution for time and consistency. Using the framework as a foundation, DHS can

- Compile initial technical competency models in a compressed timeframe
- Maintain consistency in terminology across all agencies and components, as well as alignment with NICE and OPM

What are Competency Models? – Nuts and Bolts

CYBER ROLE

Cybersecurity Tester: The Cybersecurity Tester provides compliance-based security testing leveraging automated tools. The Cybersecurity Tester assists in the preparation, development, modification, and management of security products in support of the C&A process. The Cybersecurity Tester provides technical analysis and automated scans to assess their completeness and identify system vulnerabilities and weaknesses.

CYBER SKILLS

- ▶ Systems Requirements Analysis
- ▶ Testing
- ▶ Vulnerability Assessment
- ▶ Threat Assessment
- ▶ Penetration Testing
- ▶ Certification & Accreditation
- ▶ Secure Network Design

BEHAVIORAL INDICATORS

<p>THREAT ASSESSMENT: Identifies the impact of circumstances or events with the potential to harm the enterprise architecture, networks, communications, applications, and systems. Analyzes Cyber threats to determine the</p> <p>VULNERABILITY ASSESSMENT: Uses knowledge of the types and techniques of exploitation and attack (e.g., virus, worm, Trojan horse, logic bomb, sniffers) to identify system vulnerabilities and report vulnerabilities in enterprise architecture.</p> <p>TESTING: Performs in-depth, end-to-end testing to ensure security design and development are in alignment with established security protocols, including the organization's security objectives, programming, the certification & accreditation process, and the system's security requirements.</p> <p>SYSTEMS REQUIREMENTS ANALYSIS: Translate functional security requirements into secure design technical and operational specifications. Reviews requirements documentation to determine security impact and requirements. Conducts security risk assessments and business impact analyses to detect weaknesses and depth/breadth of security controls needed. Evaluates current state of security systems, processes, and controls. Performs gap analyses and makes recommendations for gap mitigation.</p>	<p>Proficiency Level 1</p> <ul style="list-style-type: none"> ▶ Performs technical planning, system integration, verification and validation, and supportability and effectiveness analyses for total systems ▶ Analyzes all levels of total system products to include: acquisition, concept, design, test, installation, operation, maintenance, and disposal ▶ Translate operational requirements into technical requirements ▶ Organizes and analyzes stated requirements into categories throughout the system lifecycle such as functionality, usability, performance, operational, security, etc. ▶ Proficient at using a requirements management tool (e.g., DOORS) ▶ Identifies and documents security requirements 	<p>Proficiency Level 2</p> <ul style="list-style-type: none"> ▶ Leads the definition and flow-down functional, performance, and design requirements ▶ Performs functional analysis, timeline analysis, requirements allocation, and interface definition studies to translate customer requirements into hardware and software specifications ▶ Distinguishes testable requirements ▶ Conducts gap analyses between requirements and proposed architecture to identify security performance and other weaknesses in the system ▶ Verifies security requirements through collaboration with DAA/IA/Engineering & Systems Administration ▶ Conducts vulnerability & risk assessment analyses 	<p>Proficiency Level 3</p> <ul style="list-style-type: none"> ▶ Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements ▶ Interprets mission objective and applies knowledge to requirements and implementations ▶ Advises customer of gaps in security policy and guidance; provides recommendations ▶ Monitors industry developments and evolving instruction/policy/guidance on IT security concerns ▶ Oversees large-scale requirements development and management efforts to include the definition of new requirements and the implementation of changes to existing requirements.
--	---	---	--

PERFORMANCE STANDARDS

CYBER SKILL & PROFICIENCY STANDARDS	PERFORMANCE LEVEL		
	INT	EXP	FEL
Systems Requirements Analysis	2	3	3
Testing	2	3	3
Vulnerability Assessment	1	2	3
Threat Assessment	2	2	2
Penetration Testing	1	2	2
Certification & Accreditation	1	2	2
Secure Network Design	1	1	2

Applying the NICE Framework

DHS SPECIFIC CYBER ROLE

Cybersecurity Tester: The Cybersecurity Tester provides compliance-based security testing leveraging automated tools. The Cybersecurity Tester assists in the preparation, development, modification, and management of security products in support of the C&A process. The Cybersecurity Tester provides technical analysis and automated scans to assess their completeness and identify system vulnerabilities and weaknesses.

SPECIALTY AREAS

- ▶ Systems Requirements Planning
- ▶ Test and Evaluation
- ▶ Investigation
- ▶ Computer Network Defense

Selected by
Component SMEs
from NICE
Framework Specialty
Areas

BEHAVIORAL INDICATORS

THREAT ASSESSMENT: Identifies the impact of circumstances or events with the potential to harm the enterprise architecture, networks, communications, applications, and systems. Analyzes Cyber threats to determine the potential for exploitation and the impact of exploitation on the enterprise.

VULNERABILITY ASSESSMENT: Uses knowledge of the types and techniques of Cyber exploitation and attack (e.g., phishing, worms, Trojan horse, logic bomb, etc.) to identify, quantify, prioritize, and report vulnerabilities in enterprise architecture, networks, communications, applications, and systems.

TESTING: Performs in-depth, end-to-end testing to ensure secure design and development are in alignment with established security protocols, including the organization's security objectives encompassing the certification and accreditation process.

Built by SMEs with alignment to respective NICE Framework KSAs

Proficiency Level 1	Proficiency Level 2	Proficiency Level 3
<ul style="list-style-type: none"> ▶ Performs technical planning, system integration, verification and validation, and supportability and effectiveness analyses for total systems ▶ Analyzes all levels of total system products to include: acquisition, concept, design, test, installation, operation, maintenance, and disposal ▶ Translate operational requirements into technical requirements ▶ Organizes and analyzes stated requirements into categories throughout the system lifecycle such as functionality, usability, performance, operational, security, etc. ▶ Proficient at using a requirements management tool (e.g., DOORS) ▶ Identifies and documents security requirements 	<ul style="list-style-type: none"> ▶ Leads the definition and flow-down functional, performance, and design requirements ▶ Performs functional analysis, timeline analysis, requirements allocation, and interface definition studies to translate customer requirements into hardware and software specifications ▶ Distinguishes testable requirements ▶ Conducts gap analyses between requirements and proposed architecture to identify security performance and other weaknesses in the system ▶ Verifies security requirements through collaboration with DAA/IA/Engineering & Systems Administration ▶ Conducts vulnerability & risk assessment analyses 	<ul style="list-style-type: none"> ▶ Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements ▶ Interprets mission objective and applies knowledge to requirements and implementations ▶ Advises customer of gaps in security policy and guidance; provides recommendations ▶ Monitors industry developments and evolving instruction/policy/guidance on IT security concerns ▶ Oversees large-scale requirements development and management efforts to include the definition of new requirements and the implementation of changes to existing requirements.

PERFORMANCE STANDARDS

CYBER SKILL & PROFICIENCY STANDARDS	PERFORMANCE LEVEL		
	INT	EXP	FEL
Systems Requirements Planning	2	3	3
Test and Evaluation	2	3	3
Investigation	1	2	3
Computer Network Defense	2	2	2

Current challenges using NICE Framework

- Specialty Areas not “perfectly” aligned to DHS cyber roles/mission
- Limited coverage for programmatic and other roles

Current challenges: Our solutions

- Specialty Areas not “perfectly” aligned to DHS cyber roles/mission
 - Using Behavioral Indicators and proficiency levels to make models “aligned” to DHS cyber roles

Basic	Intermediate	Advanced
At this level, individuals perform behaviors that show they have fundamental knowledge/awareness of the competency. They have limited capability in applying this competency but are capable of performing tasks, applying this competency with guidance and supervision.	At this level, individuals perform behaviors that show they have substantial knowledge/awareness of the competency. They can apply the competency and are considered capable to fully perform work that requires application of this competency. These individuals are capable of demonstrating this competency in straightforward and routine situations and can contribute knowledge or new ideas in applying this competency. They implement the competency with little help and work independently most of the time.	At this level, individuals perform behaviors that show exceptional knowledge/awareness of the competency. They can synthesize/evaluate the competency and are looked to as experts in this competency. Others view these individuals as role models capable of leading or teaching others in this area, and they consult with them for assistance or guidance with work requiring this competency. These individuals obtain best-in-class results, setting the standard for performance.

Current challenges: Our solutions

- Limited coverage for programmatic and other roles
 - Provide feedback to NICE from what we gather in the field

To: Burgess, Roy (Roy.Burgess@dhs.gov)
Subject: One other piece of feedback from the field

Roy,

...so I am forwarding it to the NICE folks for their consideration, banter, decision and action as they deem appropriate.

Current Specialty Area and Definition:

Vulnerability Assessment and Management: Conducts assessments on threats and vulnerabilities, determines the level of risk, deviations from acceptable configurations, enterprise or local policy, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

Feedback/Recommendation received from CICPA on the Specialty Area and Definition:

Capability Assessment and Management: Conducts evaluations to determine the state of repeatable process, procedure, and management of IT operations delivering a critical infrastructure service. Utilizes a standard process improvement framework to determine levels of capability, maturity, and resilience of these operations, including focused inquiry of asset, technology, risk (vulnerability, threat, and consequence), continuity, dependency, and situational awareness management. Develops and/or recommends appropriate options for consideration to reduce risk exposures under normal circumstances and in times of operational stress

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



NBISETM
NATIONAL BOARD OF INFORMATION
SECURITY EXAMINERS



From cybersecurity competencies to a job performance model

David H. Tobey, Ph.D.
VP, Director of Research
National Board of Information Security Examiners

From cybersecurity competencies to a job performance model

1. The Science of Cybersecurity Competency Development

- A. Are we measuring the right things?
- B. Are we measuring the right way?
- C. Are our measures meaningful and predictive?

2. Methods, Best Practices and Challenges

A. Methods and best practices

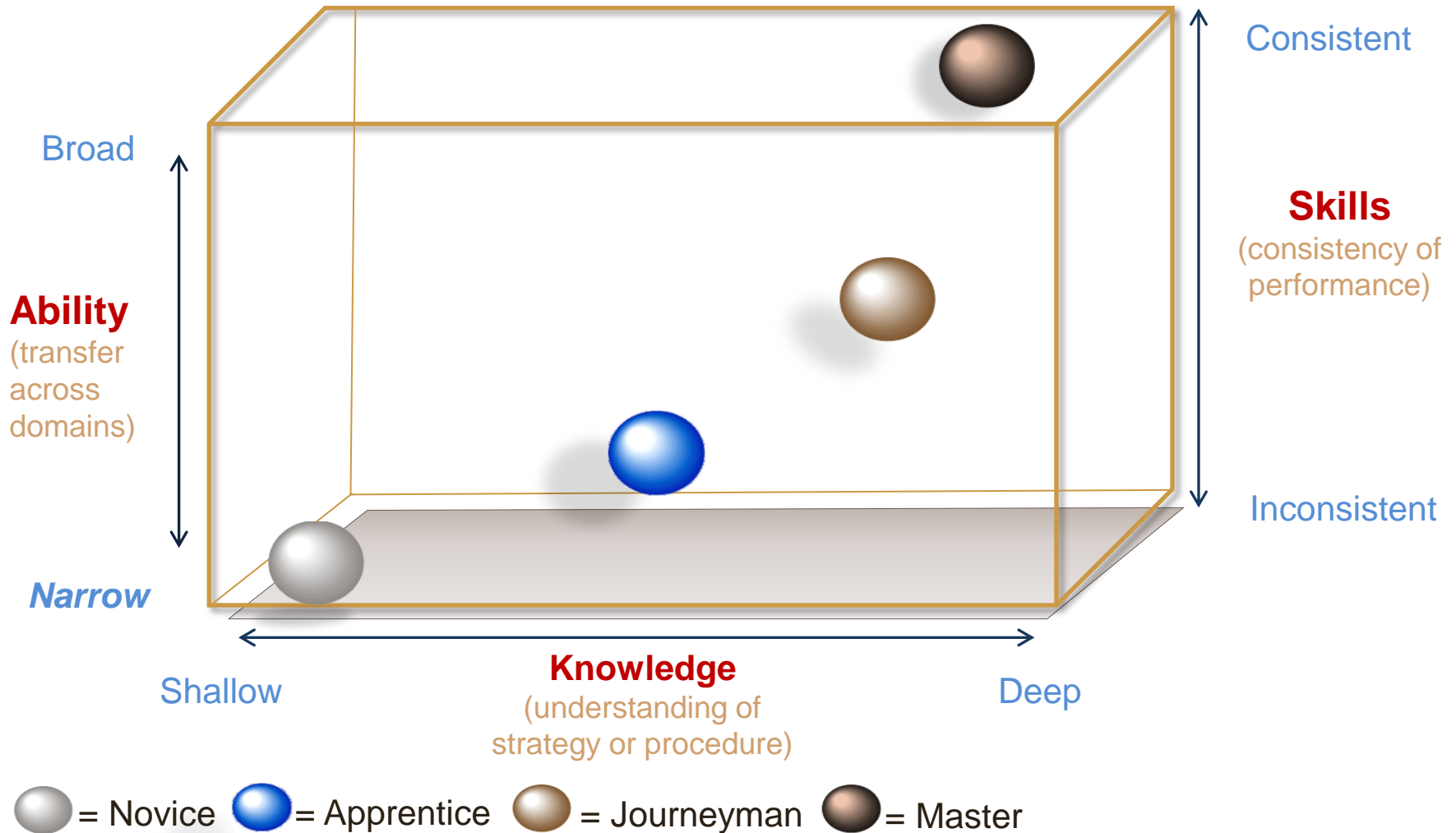
- i. Eliciting organizational context through vignettes and role/responsibility relationships
- ii. Achieving alignment through goal and objective elicitation
- iii. Defining proficiency at multiple levels for multiple roles
- iv. Identifying critical and differentiating tasks that explain differences in skill level
- v. Job Performance Models: The path from apprentice to master

B. Challenges

- i. Competency modeling at ground truth speed
- ii. Facilitating the translation of competency models into workforce development programs

3. Why Job Performance Models Are Important

What is a competency?



Source: Tobey, D. H. et. al. (2011) Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance," National Board of Information Security Examiners, Idaho Falls, ID, OST Working Group Report NBISE-OST-11-01

Are we measuring the right things?

Best Practices in Competency Modeling

Analyzing Competency Information (Identifying Competencies)

1. Considering organizational context
2. Linking competency models to organizational goals and objectives
3. Start at the top
4. Using rigorous job analysis methods to develop competencies
5. Considering future-oriented job requirements
6. Using additional unique methods

Organizing and Presenting Competency Information

7. Defining the anatomy of a competency (the language of competencies)
8. Defining levels of proficiency on competencies
9. Using organizational language
10. Including both fundamental (cross-job) and technical (job-specific) competencies
11. Using competency libraries
12. Achieving the proper level of granularity (number of competencies and amount of detail)
13. Using diagrams, pictures, and heuristics to communicate competency models to employees

Using Competency Information

14. Using organizational development techniques to ensure competency modeling acceptance and use
15. Using competencies to develop HRs systems (hiring, appraisal, promotion, compensation)
16. Using competencies to align the HR systems
17. Using competencies to develop a practical “theory” of effective job performance tailored to the organization
18. Using information technology to enhance the usability of competency models
19. Maintaining the currency of competencies over time
20. Using competency modeling for legal defensibility (e.g., test validation)

Source: Campion et al. (2011) p. 230



NBISE Job Performance Methodology

Analyzing Competency Information (methods)

- Context: Vignette Elicitation
- Goals and objectives: PRISM method
- Rigorous/Future-oriented job analysis: JTCA

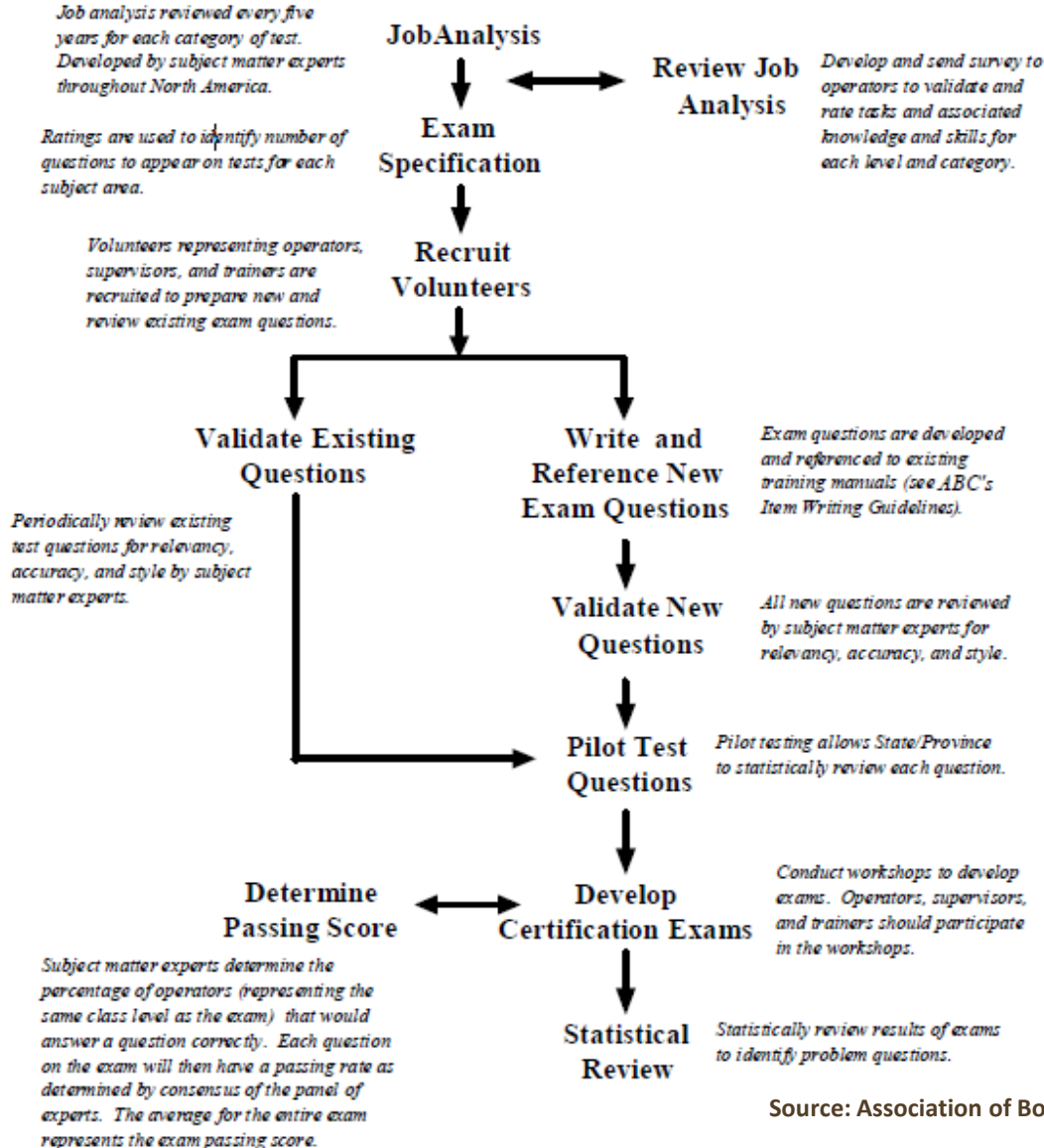
Organizing Competency Information

- Anatomy of a competency: KSA*MT
- Levels proficiency: JAQ – multiple performance levels for multiple roles
- Org. Language/Hard/Soft Skills: technical and operational tasks prescribed by methods
- Level of analysis: KSA Quadrant analysis
- Diagrams: Predictive Performance Model (PPA)
- Competency libraries: ADAPTS

Facilitating use of Competency Information:

Establish standards based on validated curricula, assessment, and simulation libraries

Are we measuring the right way?



NBISE Job Performance Methodology

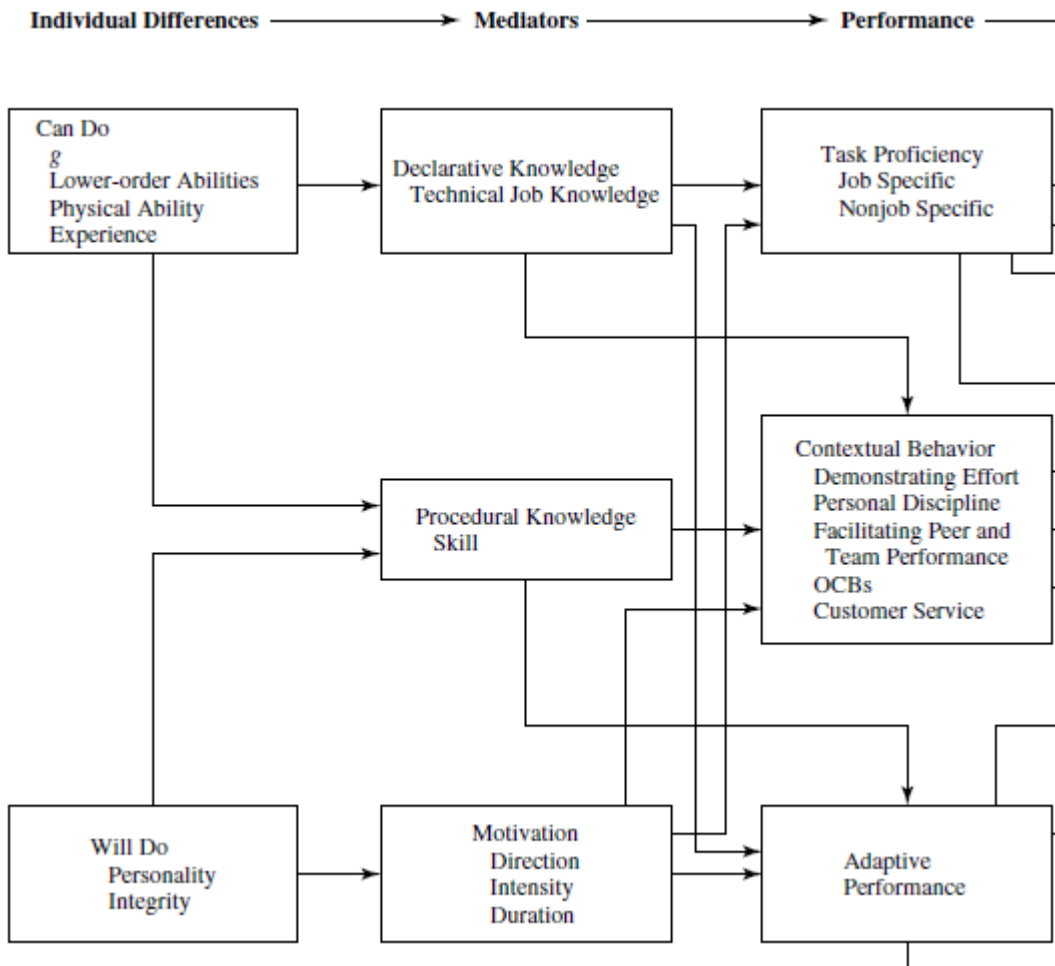
Not all validation is the same

Most competency model or assessment validations focus on whether the model statements and assessment questions relate to the job and are fair; rather than that they identify the critical elements that are predictive of job performance.

Validating construct and predictive validity

- Item Difficulty Index
- Item Discrimination Index
- Distractor Analysis
- Homogeneity Analysis
- Reliability Index

Are the measures meaningful and predictive?



NBISE Job Performance Methodology

Predictors of Performance

- Situational judgment
- Behavioral consistency

Achievement vs. Aptitude Assessment

- Achievement tests measure the **proficiency** of recall of past knowledge. These tests are **descriptive** – they classify people into categories based on the depth of understanding of a domain. They measure the observed score on a test.
- Aptitude tests measure future **potential**. These tests are considered **predictive** – forecasting how the tested individual can be expected to perform. These tests seek to separate knowledge from skill from ability. They use adaptive testing techniques and statistical analyses to measure the true score on a test.

Source: Schmitt, Cortina, Ingerick & Wiechmann (2003), p. 79

Eliciting organizational context through vignettes

Vignettes	Security Operations Center Role	IT Security Role	Network Administration Role	Incident Handling Role
<p>START HERE >>></p> <p>Vignette: A new security vulnerability has been announced that affects your organization, such as a Microsoft vulnerability.</p>	<ol style="list-style-type: none"> 1. Update relevant detection mechanisms (eg IDS signatures) 2. Ensure operational procedures updated to respond to new alerts 3. Situational awareness of emerging threats related to the vulnerability 4. Coordinate with the firewall, network, antivirus and intrusion detection teams to understand the signature coverage, status of vulnerability scans, firewall blocks in place etc. 5. Develop a notification / alert to be disseminated to all relevant parties. 6. Monitor logs and IDS for new compromises that may be related to this new vulnerability 	<ol style="list-style-type: none"> 1. Oversee patching process 2. Coordinate with application administrators, system administrators for patch testing and deployment. 3. Assist in determining patch release timelines based on associated risk. 4. Implement associated security mitigations, such as intrusion detection signatures, host-based intrusion detection signatures and controls 5. Create new rules in security tools to watch for new compromises exploiting this new vulnerability 	<ol style="list-style-type: none"> 1. Implement mitigating controls related to network infrastructure (eg, potentially a firewall/proxy/router block) 2. Implement firewall blocks, router ACLs, ensure bandwidth SLAs, review router/firewall logs for suspicious traffic 3. Implement new network mitigations related to this vulnerability 	<ol style="list-style-type: none"> 1. Prepare to respond to any incidents related to exploitation of the vulnerability 2. Respond to new compromises
<p>Vignette: Data exfiltration: Company information / operations leaking to outside actor</p>	<ol style="list-style-type: none"> 1. Update relevant detection mechanisms (eg IDS signatures) 2. Ensure operational procedures updated to respond to new alerts 3. Reviewing all sources of information relating to the data leakage to determine extent, time, location, etc. 4. Monitor for exfiltration 	<ol style="list-style-type: none"> 1. Evaluate recommendations in post mortem 2. Mitigate exfiltration and update security tools to monitor for exfiltration attempts 	<ol style="list-style-type: none"> 1. Implement mitigating controls related to network infrastructure (eg, potentially a firewall/proxy/router block) 2. Assist in data gathering/monitoring 3. Collect network information, netflow, router logs to assist in response. 4. Apply mitigations to firewalls and other network devices 	<ol style="list-style-type: none"> 1. Determine scope of incident (number of systems, which data, etc) 2. Determine response plan (when to remediate, how to remediate) 3. Oversee remediation effort 4. Interface with law enforcement 5. Determine root cause 6. Coordinate with all other parties to identify, contain and mitigate the data loss. 7. Research how the attackers were able to compromise system to exfiltrate data, mitigate, and report findings on what information was exfiltrated

Source: Tobey, D. H. (2011) A competency model of advanced threat response. National Board of Information Security Examiners, Idaho Falls, ID, ATR Working Group Report NBISE-ATR-11-02

Eliciting context through overlapping roles/responsibilities

Update overarching policies and procedures	Security Operations Center Role	IT Security Role	Network Administration Role	Incident Handling Role
Ensure procedures address Phishing				
Task ==>	Review SOP created by IT Security for detection and response	Create definitions for the different types of phishing attacks	Review SOP created by IT Security for detection and response	Review SOP created by IT Security for detection and response
Task ==>	Implement the SOP created by IT Security for detection and response	Determine steps to respond to the various phishing attacks	Work with IT Security on the feasibility of the mitigations	Provide lessons learned feedback to IT Security as the SOP is followed and needs modifications
Task ==>	Refer to the end-user training to educate end-users who call in	Create end-user training	Work with IT Security to update the SOP as new technologies are implemented	
Task ==>		Create SOP for responding to and mitigating phishing attacks		
Task ==>				
INSERT ROWS ABOVE THIS LINE AS NEEDED				
Policy/procedure definition to clarify process owner				
Task ==>	Work with the other roles to determine the various processes and who should own them	Take the lead on working with the other roles to determine the various processes and who should own them	Work with the other roles to determine the various processes and who should own them	Work with the other roles to determine the various processes and who should own them
Task ==>	Create the process documentation for the Security Operations Center Role	Create the process documentation for the IT Security Role	Create the process documentation for the Network Administration Role	Create the process documentation for the Incident Handling Role
Task ==>	Review process documentation with the other roles	Review process documentation with the other roles	Review process documentation with the other roles	Review process documentation with the other roles
Task ==>	Obtain buy-in from the other roles on the Security Operations Center processes	Obtain buy-in from the other roles on the IT Security processes	Obtain buy-in from the other roles on the Network Administration processes	Obtain buy-in from the other roles on the Incident Handling processes
Task ==>		Lead an annual process documentation review for all roles		

Source: Tobey, D. H. (2011) A competency model of advanced threat response. National Board of Information Security Examiners, Idaho Falls, ID, ATR Working Group Report NBISE-ATR-11-02

Achieving alignment through goal/objective elicitation (PRISM)

Goal	Priority	Objective measure	PRISM ==>			<== PRISM	
			Premier	Robust	Improved	Satisfactory	Moot
Update overarching policies and procedures	Primary	The time frame policies and procedures are updated to reflect the changing threat landscape	Policies and procedures are updated in real time as incidents are worked and new threats are discovered	Policies and procedures are updated weekly to reflect incidents worked that week and new threats discovered that week	Policies and procedures are updated monthly to reflect incidents worked that month and new threats discovered that month	Policies and procedures are updated every 6 months to reflect incidents worked during the previous 6 month period and new threats discovered during that same 6 month period	Policies and procedures are updated annually to reflect incidents worked during the year and new threats discovered during the year
Perform gap analysis of ability to detect or identify vulnerable systems	Primary	Time frame required to determine gaps	Gap analysis performed within 1 hour of vulnerability notification	Gap analysis performed within 2 hours of vulnerability notification	Gap analysis performed within 4 hours of vulnerability notification	Gap analysis performed within same working day of vulnerability notification	Gap analysis performed after 24 hours
Classify data properly and regularly review	Secondary	Percentage of data classified Frequency of review	100% of data classified and reviewed monthly	90% of data classified and reviewed quarterly	75% of data classified and reviewed bi-annually	50% of data classified and reviewed annually	25% of data classified and no formal review process
Monitoring sources for vulnerability notices and changes in the threat environment	Primary	Person/Resource assigned task to monitor sources	Dedicated threat intelligence team Automated solution to monitor and provide information automatically to team based on asset profiles, or risk profiles of members	Dedicated threat intelligence resource Automated solution to monitor and provide information automatically to team	Resource assigned additional threat intelligence responsibility Automated solution to monitor and provide information for manual review	Automated solution to monitor and provide information for review	No resources to monitor
Respond to intrusion events	Primary	Monitor security events real time	24x7 security staff monitor security events real time	8x5 security operations staff monitor events near real time	Security events are sent to personnel automatically near real time	Security events are reviewed manually as time permits	No capability to monitor security events

Source: Tobey, Wanasika & Chavez (2007) "PRISM: A goal-setting , alignment and performance evaluation exercise. Proceedings of the Organizational Behavior Teachers Conference, Malibu, CA.

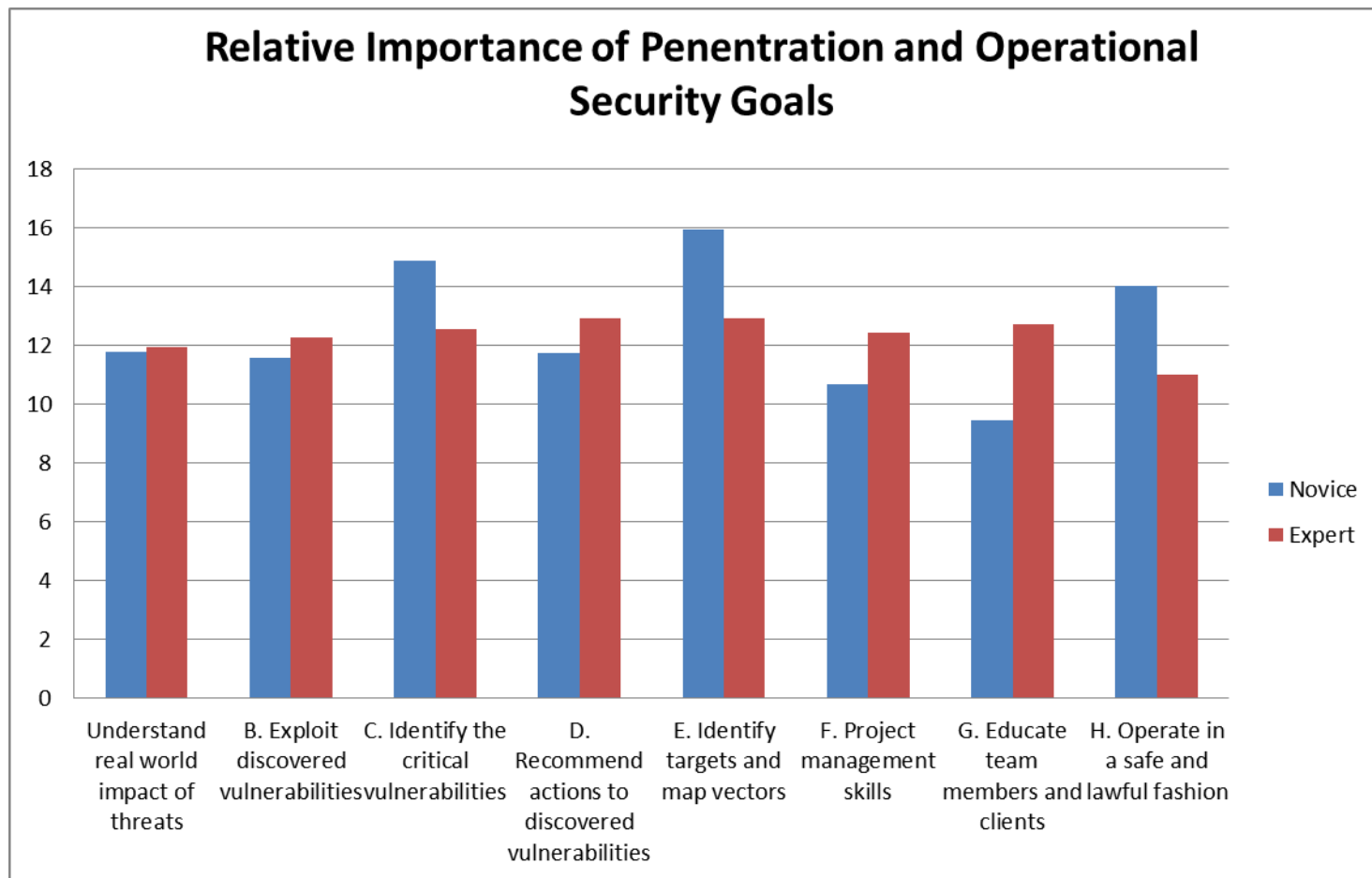
Defining proficiency at multiple levels for multiple roles

1. How important is it that a person at the listed level of expertise, or filling the listed job role, be skilled at accomplishing this task?

	Entry Level (Apprentice): 1:Unimportant 2:Low 3:Moderate 4:Very 5:Extremely	Intermediate (Journeyman): 1:Unimportant 2:Low 3:Moderate 4:Very 5:Extremely	Expert Level (Master): 1:Unimportant 2:Low 3:Moderate 4:Very 5:Extremely	Commercial Pentester: 1:Unimportant 2:Low 3:Moderate 4:Very 5:Extremely	Red Team: 1:Unimportant 2:Low 3:Moderate 4:Very 5:Extremely	Blue Team: 1:Unimportant 2:Low 3:Moderate 4:Very 5:Extremely
1. Develop strategies for local traffic analysis	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
2. Develop mission/attack plan to assess security posture of client/target network	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
3. Use nontraditional problem solving skills to solve complex problems	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
4. Apply filters to pull the correct protocols and ports	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
5. Develop an understanding of TCP/IP flow	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
6. Use packet captures to determine if a service is alive	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
7. Capture legit websites; add instrumentation for redirection and exploitation	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
8. Map the route between the engagement point and target(s)	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
9. Analyze e-mail communication for information leakage	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
10. Analyze active directory information	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
11. Interpret error messages	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
12. Map web server directory structure	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
13. Identify targets for planned attacks	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
14. Identify ownership of gateway devices	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
15. Attack vectors associated with error messages	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5

Source: Tobey, D. H. et. al. (2011) Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance," National Board of Information Security Examiners, Idaho Falls, ID, OST Working Group Report NBISE-OST-11-01

Identifying indicators that differentiate skill levels



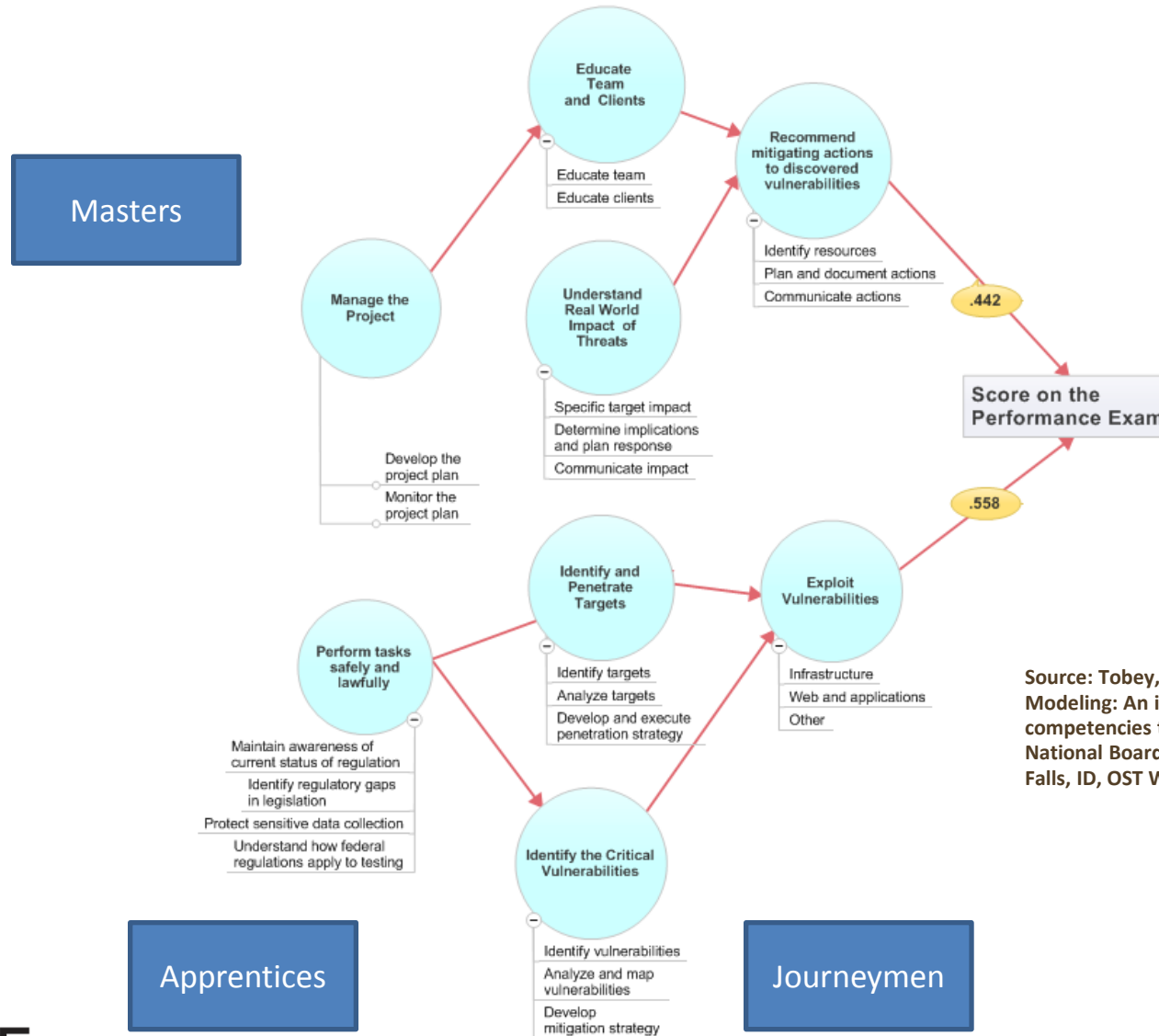
Source: Tobey, D. H. et. al. (2011) Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance," National Board of Information Security Examiners, Idaho Falls, ID, OST Working Group Report NBISE-OST-11-01

Identifying indicators that differentiate skill levels

		CRITICALITY
		HIGH
D I F F E R E N T I A T I O N	H i g h	<ol style="list-style-type: none"> 1. Recognize when tools provide inaccurate data 2. Multi-task between multiple phases of testing 3. Develop mission/attack plan to assess security posture of client/target network 4. Identify vulnerable network aware appliances on the target network. 5. Ensure all project goals and objectives are clear to team 6. Explain results of attacks to clients 7. Identify targets for potential exploitation 8. Establish control of Windows machines 9. Communicate best practices in security to clients 10. Identify major attack targets and assets 11. Identify specific vulnerabilities on identified hosts 12. Escalate privileges on an Active Directory network 13. Utilize pass the hash to compromise additional systems and privilege escalation to gain root access of a system. 14. Compromise individual host or service 15. Understand and attack standard data protection mechanisms 16. Survey environment to develop situational awareness of the environment. 17. Establish control of remote access mechanisms from inside 18. Demonstrate robust post-exploitation capability 19. Analyze data found on compromised machines for strategic value as seen by a worst case actual attacker 20. Analyze data found on compromised machines to enable exploitation deeper into the network. 21. Exploit web applications 22. Educate others to translate the cyberrisk to operational risk.

Source: Tobey, D. H. et. al. (2011) Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance," National Board of Information Security Examiners, Idaho Falls, ID, OST Working Group Report NBISE-OST-11-01

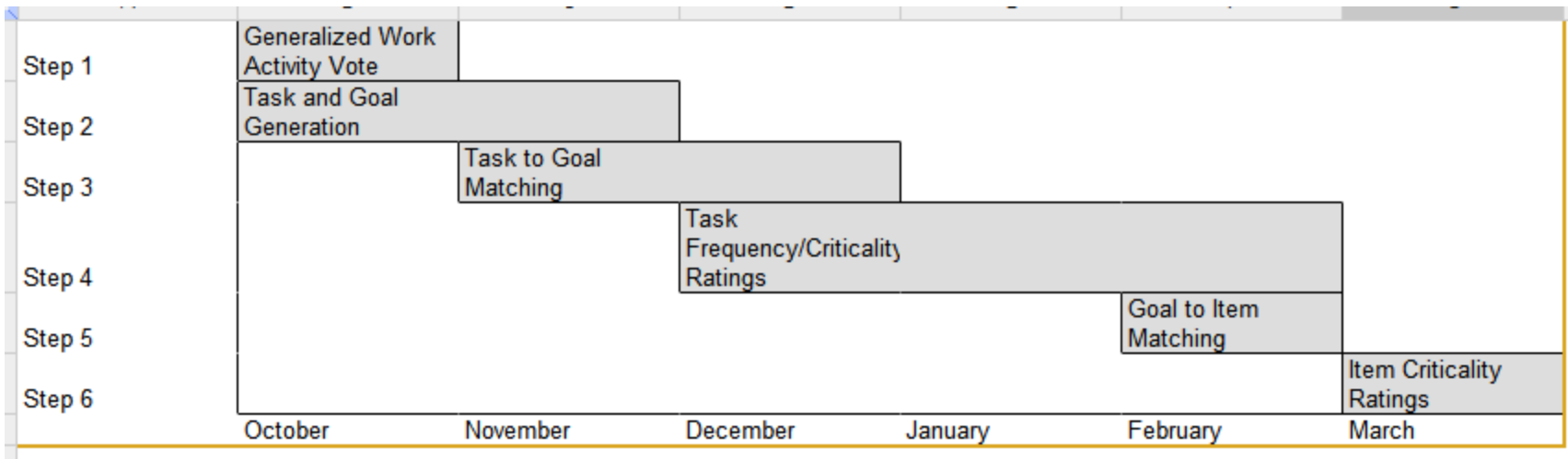
Defining the path to performance



Source: Tobey, D. H. et. al. (2011) Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance," National Board of Information Security Examiners, Idaho Falls, ID, OST Working Group Report NBISE-OST-11-01

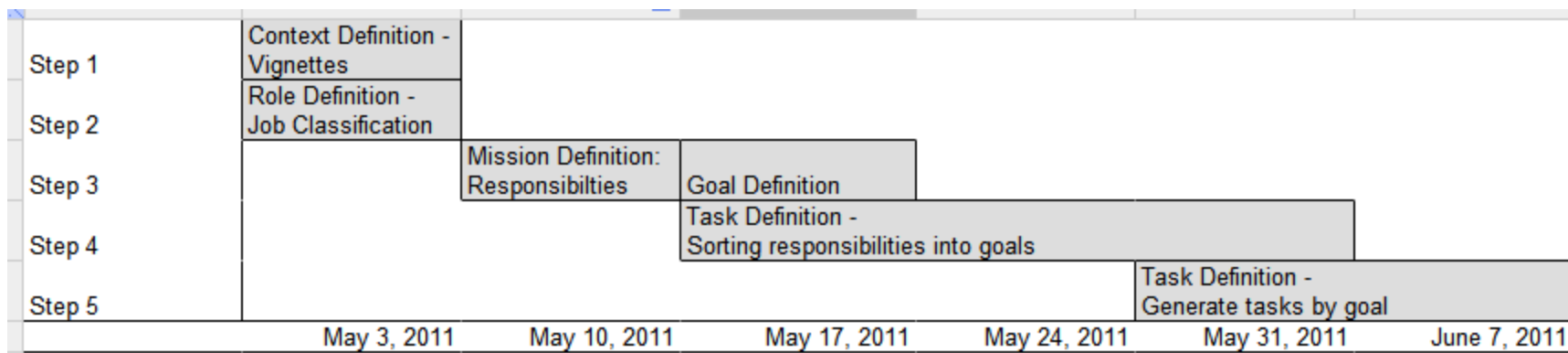
Challenge 1: Competency modeling at ground truth speed

Process based on O*NET methodology



Challenge 1: Competency modeling at ground truth speed

Process based on critical incident elicitation methodology



Challenge 2: Facilitating alignment - The case of ATR

The 31 Cybersecurity Specialties:

Securely Provision

- Systems Requirements Planning
- Systems Development
- Software Engineering
- Enterprise Architecture
- Test and Evaluation
- Technology Demonstration
- Information Assurance Compliance

Operate and Maintain

- System Administration
- Network Services
- Systems Security Analysis
- Customer Service and Technical Support
- Data Administration
- Knowledge Management
- Information Systems Security Management

Support

- Legal Advice and Advocacy
- Education and Training
- Strategic Planning and Policy Development

Protect and Defend

- Computer Network Defense Infrastructure Support
- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense Security Program Management

Investigate

- Investigation
- Digital Forensics

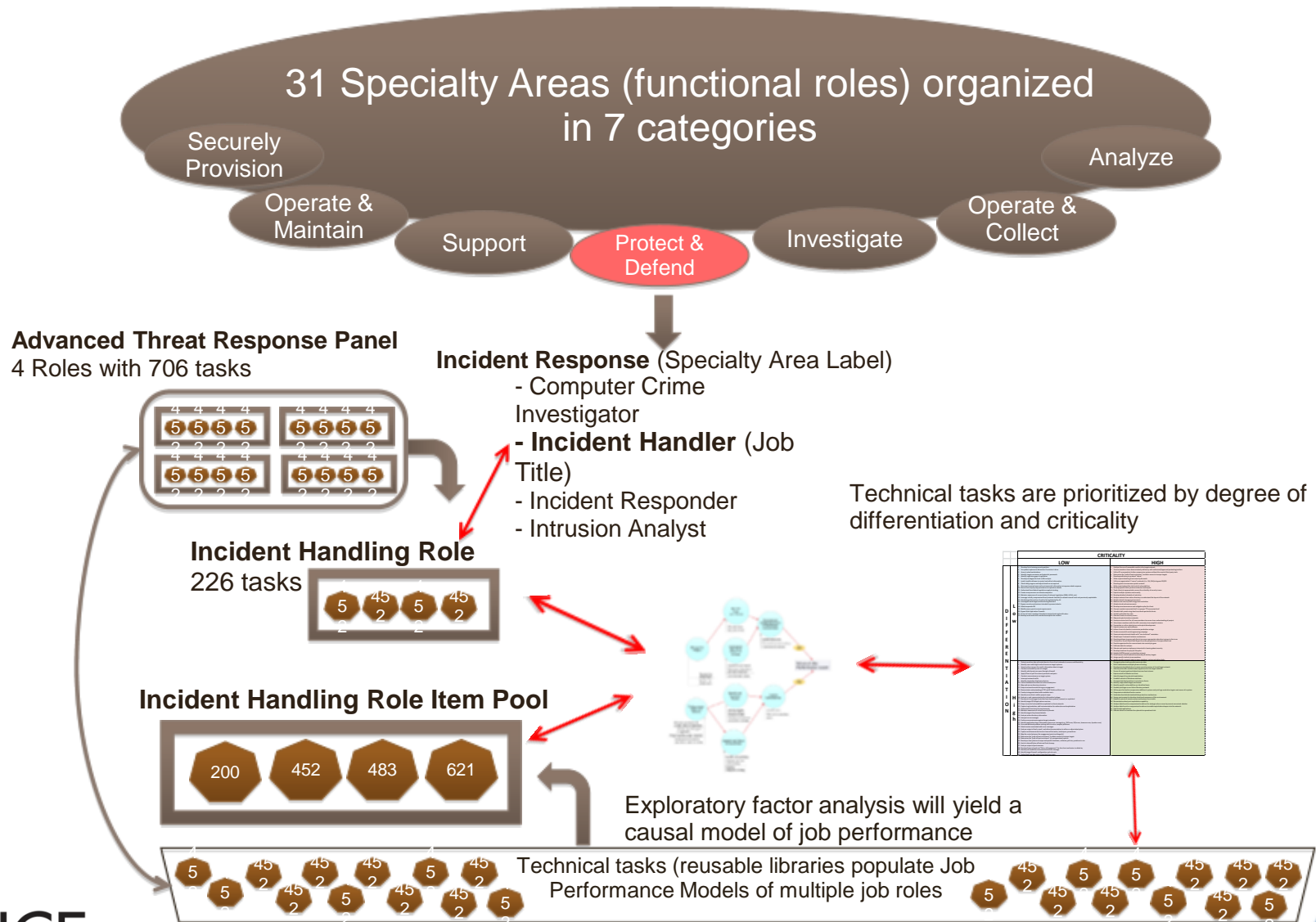
Operate and Collect

- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Analyze

- Cyber Threat Analysis
- Exploitation Analysis
- Targets
- All Source Intelligence

Challenge 2: Achieving alignment - The case of ATR



Why job performance models are important

- ❑ Facilitate translation of functional roles into job roles
- ❑ Clearly distinguish knowledge, skill, and ability
- ❑ Determine factors that differentiate performance at varying levels of skill
- ❑ Identify the critical factors that predict performance
- ❑ Competency models **describe**
Job performance models **prescribe**

JPM's help to determine who should be developed (*aptitude*), how to development them (*skill profiles*), and when they are ready to take the next step (*performance-based learning*)

THE FAR SIDE by Gary Larson



"Mr. Osborne, may I be excused? My brain is full."

Discussion

Thoughts

- How might the Framework be applicable to a staffing challenge you are facing?
- What could be the best method to evaluate individual cybersecurity competency (e.g. testing, hands-on application, etc.)?
- How might your organization make use of and benefit from a competency assessment methodology?

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



Determining Current Cybersecurity Capabilities

Develop and maintain an unrivaled, globally competitive cybersecurity workforce