



U.S. DEPARTMENT OF  
**ENERGY**

PNNL- 22653

Prepared for the U.S. Department of Energy  
under Contract DE-AC05-76RL01830

# Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs for Phase 2 of the Secure Power Systems Professional project

LR O'Neil  
MJ Assante  
DH Tobey  
TJ Conway

TJ Vanderhorst, Jr  
J Januszewski, III  
R Leo  
K Perman

August 2013



**Pacific Northwest**  
NATIONAL LABORATORY

*Proudly Operated by **Battelle** Since 1965*

## DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY

*operated by*

BATTELLE

*for the*

UNITED STATES DEPARTMENT OF ENERGY

*under Contract DE-AC05-76RL01830*

Printed in the United States of America

Available to DOE and DOE contractors from the

Office of Scientific and Technical Information,

P.O. Box 62, Oak Ridge, TN 37831-0062;

ph: (865) 576-8401

fax: (865) 576-5728

email: [reports@adonis.osti.gov](mailto:reports@adonis.osti.gov)

Available to the public from the National Technical Information Service

5301 Shawnee Rd., Alexandria, VA 22312

ph: (800) 553-NTIS (6847)

email: [orders@ntis.gov](mailto:orders@ntis.gov) <<http://www.ntis.gov/about/form.aspx>>

Online ordering: <http://www.ntis.gov>



This document was printed on recycled paper.

(8/2010)

# **Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs for Phase 2 of the Secure Power Systems Professional project**

LR O’Neil  
MJ Assante  
DH Tobey  
TJ Conway

TJ Vanderhorst, Jr  
J Januszewski, III  
R Leo  
K Perman

Contributors:  
SGC Panel Members

August 2013

Prepared by:  
Pacific Northwest National Laboratory and  
NBISE Secure Power Systems Professional Project Team

A summary version of this report titled: *Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs—Summary Report for Phase 2 of the Secure Power Systems Professional project* August 2013, document clearance number PNNL- 22641 is available from [lro@pnnl.gov](mailto:lro@pnnl.gov) or [www.nbise.org](http://www.nbise.org)



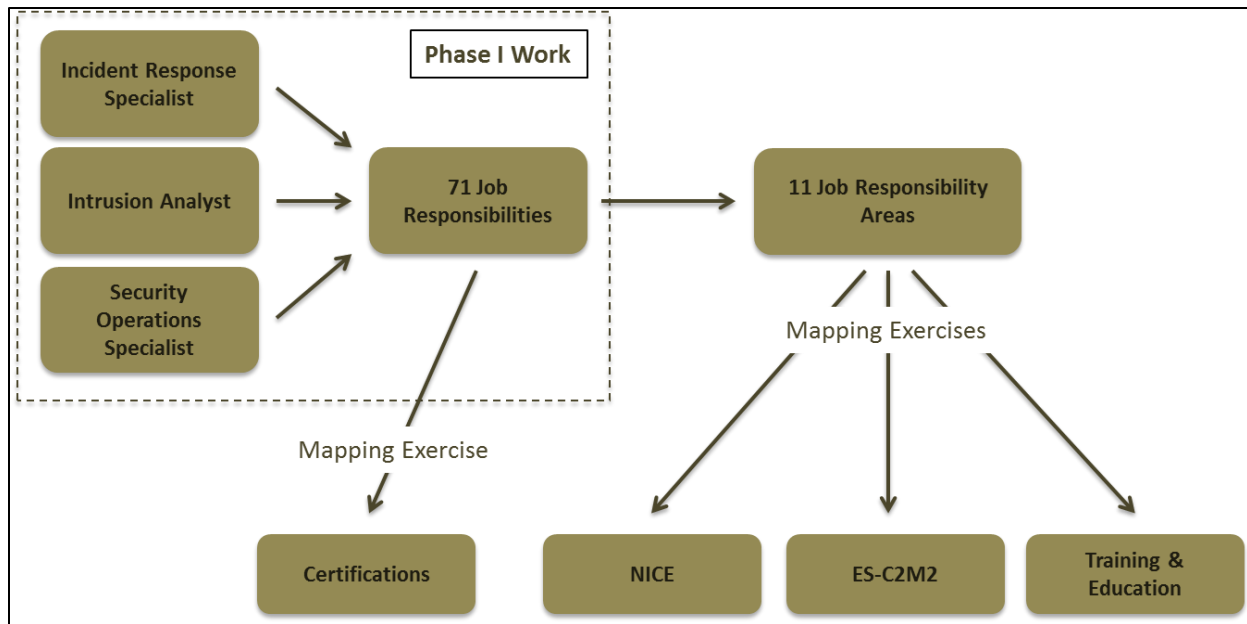
# Summary

The U.S. Department of Energy has recognized that the electric power industry needs workforce development resources that can aid in the accelerating need for Secure Power Systems Professionals, while at the same time identifying capabilities and competencies to protect and enable the modernized grid currently being built. In the spring of 2011 a project was initiated by Pacific Northwest National Laboratory with the National Board of Information Security Examiners for the U.S. Department of Energy to identify those capabilities and competencies along with assessing the need and qualifications for a certification program for Secure Power Systems Professionals. The first phase of this three-phase project was to identify operational security functions for day-to-day power systems operations (but not development, engineering, and architecture), and power system environments. The project examined the technical, problem-solving, social and analytical skills identified by stakeholders as used by existing power systems cybersecurity staff in the daily execution of their responsibilities resulting in a comprehensive Job Performance Model (JPM) for Smart Grid (O’Neil et al. 2012).

The second phase of the project applied the JPM to ascertain the alignment and gaps among existing workforce development programs. The JPM from Phase 1 included 82 job responsibilities; 71 of these responsibilities were assigned by the Smart Grid Cybersecurity Subject Matter Expert panel to 11 job responsibility areas. These responsibility areas became the basis for studying the gaps and overlaps between four cybersecurity workforce development programs:

1. the National Initiative for Cybersecurity Education National Cybersecurity Workforce Framework (NICE 2012);
2. the Energy Systems Cybersecurity Capability Maturity Model (DOE 2013a);
3. power systems cybersecurity education courses; and
4. cybersecurity certifications (Figure S.1).

The Subject Matter Expert panel’s findings were validated through a public survey: both the panel’s findings and the survey identified responsibility areas lacking sufficient coverage in the currently available workforce programs.



**Figure S.1. Mapping Job Responsibilities and Workforce Development Resources**

The analysis of certifications yielded nine vendor-neutral certifications that panel members indicated were valuable for determining job competence (Figure S.2). The results indicate that no single certification exists for a Secure Power Systems Professional. A combination of certifications has value in determining a base level of competence or for enhancing an existing employee’s knowledge base. For example, someone with a North American Electric Reliability Corporation System Operator Certification could expand their cybersecurity knowledge and verify it by obtaining a cybersecurity centric certification such as one listed in Figure S.2. *Rather than trying to force existing certifications to meet the needs of the modern power grid, it is the recommendation of the panel to develop a Secure Power Systems specific certification.*

Certification	Organization
Certified Information Systems Security Professional (CISSP)	(ISC) <sup>2</sup>
System Operator Certification (SOC)	NERC
Certified Ethical Hacker (CEH)	EC-Council
Certified information Security Auditor (CISA)	ISACA
Certified Information Security Manager (CISM)	ISACA
Certified in Risk and Information Systems Control (CRISC)	ISACA
Certified Incident Handler (GCIH)	GIAC
Certified Intrusion Analyst (GCIA)	GIAC
Penetration Tester (GPEN)	GIAC
Web Application Penetration Tester (GWAPT)	GIAC

**Figure S.2. Valuable Vendor-Neutral Certifications**

The results also identified that there were very few educational offerings with a focus on cybersecurity for power systems. We did find special courses and seminars, usually within Computer Science or Electronics departments or offered by organizations such as SANS<sup>1</sup> or ISA (Internal Security

<sup>1</sup> <http://www.sans.org/>

Associates), but not any courses related to cybersecurity in power engineering programs as part of a college or vocational program to graduate work-ready employees. Cybersecurity of power systems education needs to be available to college students now so that they are ready to defend and protect the modern power grid when they graduate and enter the workforce.

There are several useful conclusions that can be implemented by stakeholders immediately:

1. Entities can use the job roles identified as having a strong alignment with applicable certifications to adjust job postings or staff development programs to align with identified job roles.
2. For the areas where strong alignment with an existing certification does not exist, entities can first adjust job descriptions and career paths to remove credential requirements that do not align with job-identified roles.
3. Organizations can begin developing or working with partners to utilize existing or develop new training programs that best fill the identified gaps.

“I believe these results confirm a common belief within [power and utility] entities that; traditional IT roles are fairly well defined with credentials and available credentials, while Operations Technology roles do not have a well-defined alignment to existing [cybersecurity] programs.”  
- **Tim Conway**, Panel Chair

It is recommended that work continue to validate the predictive accuracy of the JPM developed in Phase I of this project and to apply the validated model to accredit workforce programs based on job role(s), responsibility areas and expertise levels at which they are targeted. We also recommend the development of self-assessment tools to help organizations determine whether they have a holistic approach to workforce development and if they don't, how to implement one.

Panel members have indicated that a certification would be well received and a smart community investment. The continued implementation of digital technology into every aspect of power systems helps us reach the goal of a fully integrated power system without boundaries—from end to end, generation to distribution. It is incumbent on power system stakeholders to lead the effort to redefine critical power system job functions and expand those job functions to develop a workforce that can tackle the cybersecurity challenges of the country's new edgeless power system.





## Acronyms and Abbreviations

CATF	Cyber Attack Task Force
CEH	Certified Ethical Hacker
CISSP	Certified Information Systems Security Professional
CISM	Certified Information Security Manager
CSIS	Center for Strategic and International Studies
EC-Council	International Council of Electronic Commerce Consultants
ES-C2M2	Energy Systems Cybersecurity Capability Maturity Model
GIAC	Global Information Assurance Certification
GCIA	GIAC Certified Intrusion Analyst
ICS	industrial control systems
(ISC) <sup>2</sup>	International Information Systems Security Certification Consortium, Inc.
IT	information technology
JPM	Job Performance Model
NBISE	National Board of Information Security Examiners
NERC	North American Electric Reliability Corporation
NICE	National Initiative for Cybersecurity Education
OT	operational technology
PNNL	Pacific Northwest National Laboratory
RaCS	Review and Comment System
SCADA	supervisory control and data acquisition
SGC	Smart Grid Cybersecurity
SME	subject matter expert
SOC	System Operator Certification
TTP	tactics, techniques, and procedures



# Contents

1.0	Introduction .....	1.1
1.1	Impetus for the Study .....	1.1
1.2	Study Purpose and Contribution .....	1.4
1.3	Previous Work in Competency Models and Workforce Development .....	1.10
2.0	Method.....	2.1
2.1	Panel Composition .....	2.1
2.2	Panel Activities .....	2.1
2.3	Review and Comment System .....	2.1
2.4	Agreement Analyses .....	2.2
3.0	Findings .....	3.1
3.1	Certifications Mapped to Job Responsibilities .....	3.2
3.1.1	Discussion of Certification Review Results .....	3.3
3.2	Competency Frameworks and Course Topics .....	3.5
3.2.1	Discussion of Responsibility Area Mappings .....	3.6
3.3	Combined Panel and Public Responsibility Area Mappings.....	3.6
3.3.1	Discussion of Public Review and Comment System Results.....	3.7
3.4	Relative Emphasis on Critical and Differentiating Job Responsibilities.....	3.8
4.0	General Discussion .....	4.1
4.1	Review of Results by Panel Leadership .....	4.1
5.0	Implications .....	5.1
5.1	Implications for Electric Power Sector Entities .....	5.1
5.2	Implications for Competency Frameworks and Workforce Development.....	5.6
5.3	Implications for Further Research.....	5.7
6.0	Conclusion .....	6.1
7.0	References .....	7.1
	Appendix A – Smart Grid Cybersecurity (SGC) Panel Roster .....	A.1
	Appendix B – Panel Meetings and Activities for Phase 2 .....	B.1
	Appendix C – Certifications and Rating Results .....	C.1
	Appendix D – Module Public Participant Demographics.....	D.1
	Appendix E – Results and Analysis of Targeted Workforce Program Mapping to Job Responsibility Areas.....	E.1
	Appendix F – Inter-Rater Reliability for SPSP Phase 2 .....	F.1
	Appendix G – Knowledge Areas and Understanding Demonstrated for Each Certification.....	G.1
	Appendix H – Job Responsibilities and Responsibility Areas.....	H.1
	Appendix I – Assignment of Certifications to Job Responsibilities .....	I.1
	Appendix J – Mapping of Competency Model Frameworks and Course Topics to Responsibility Areas.....	J.1

Appendix K – Review and Comment System Instructions.....	K.1
Appendix L – Panel Votes Assigning Job Responsibilities to Job Roles .....	L.1
Appendix M – Education and Training Courses Identified in Open Source Search.....	M.1

## Figures

1.1. Five Pillars of the Electricity Sector .....	1.2
1.2. Examples of Electricity OT.....	1.3
1.3. Phase 2 Mappings .....	1.8
1.4. Energy OT Systems Lifecycle .....	1.9
3.1. Valuable Vendor-Neutral Certifications .....	3.1
3.2. Mapping to Responsibility Areas.....	3.5
3.3. Target Workforce Program Emphasis of Responsibility Areas .....	3.7
4.1. Greatest Coverage of Job Responsibility Areas through Implementing Combinations of Workforce Frameworks .....	4.2
5.1. Workforce Stages.....	5.2

## Tables

3.1. Vendor-Neutral Certifications Related to Job Roles.....	3.2
3.2. Certifications Associated with Job Roles.....	3.3
3.3. Job Role Coverage by Certification .....	3.4
3.4. Coverage of Responsibility Areas in the Competency Frameworks and Course Topics.....	3.6
3.5. Comparison of Fundamental and Differentiating Emphasis in Workforce Programs .....	3.9

# 1.0 Introduction

## 1.1 Impetus for the Study

The United States has embarked on a distributed and large-scale program to further modernize and expand power systems from generation to delivery. The addition of digital technology and enhanced communications is changing the face of utility operations and will result in a highly adaptable, efficient, and demand-driven power system. Technology is being used to address many of the identified challenges that can hamper system reliability and efficiency. These advances have created their own set of challenges for power utilities and power system stakeholders. The specter of an insufficient level of cybersecurity has threatened progress toward achieving modernization goals and may result in realizing greater risk inherent in implementing highly interconnected digital technology.

Modernization efforts have created increased demand for technology-centric professions from designers and programmers to technology managers. This demand includes the need for cybersecurity competence across technology roles and across a diverse set of cybersecurity-focused functional roles. This demand also cuts across the energy chain including energy system technology providers, integrators, implementers, and electric power asset owners and operators. The specific nature of performing cybersecurity related work and integrating cyber realities into traditional power system functions and job roles is not well documented or understood. A relatively new set of regulations are aimed at levying requirements against registered entities possessing bulk electric power assets in an attempt to manage some of the risks represented by cyber threats.

The myriad of electric power system stakeholders are beginning to recognize that cybersecurity is an essential part of a technology-reliant power system and a lack of security will impact system reliability, availability and safety. The North American power system is made up of thousands of generation stations and many thousands of miles of delivery lines that are operated in concert by engineering, automation, and a combination of local and centralized decision making. Technology has played a key role in unlocking additional capacity and in reducing events that result in system outages and reducing the time required to recover from outages. Cyber vulnerabilities have increased with the need to interconnect systems and share valuable data to support decisions and act more quickly with greater precision. These vulnerabilities and an expanded attack surface require a capable and competent cybersecurity workforce across the various organizations that contribute to and compose the North American power system.

Technology has become integral in changing the face of power systems. Consequently, the very definition of the components of a power system may need to be expanded from the traditional “Generation, Transmission, and Distribution” model to now include “Markets” and “Information and Communications Technology” (Figure 1.1). The industry has identified the risk associated with both the nature of cybersecurity and the challenges of recruiting, developing, and retaining a competent cybersecurity workforce. These challenges need to be addressed in parallel with modernization projects. There is an increasing gap between the need for a competent workforce to address both known and emerging cybersecurity challenges and the labor pool to fill this need (Assante and Tobey 2011). Without a viable workforce for cybersecurity, grid modernization and smart grid initiatives could be greatly hampered. Specifically, the special application of available cybersecurity professionals poses unique

challenges for operational technology (OT). (See Figure 1.2 for some examples of electric power system OT)<sup>1</sup>



**Figure 1.1.** Five Pillars of the Electric Power Sector

<sup>1</sup> OT is an umbrella term used for various technologies that support “operations,” such as SCADA Energy Management System. This term can be more inclusive than Industrial Control Systems (ICS) control systems and can include market systems that interface directly through technology with operational assets. (See Figure 1.3).



**Industrial Control Systems (ICS):** A term used to encompass the many applications and uses of industrial and facility control and automation systems. ISA-99/IEC 62443 is using Industrial Automation and Control Systems (ISA-62443.01.01) with one proposed definition being ‘a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.’

Types of Industrial/facility Automation & Control	Uses & Applications	Examples
SCADA & EMS – Supervisory Control & Data Acquisition & Energy Management System	Control and data acquisition over large geographic areas	Electricity transmission & distribution
DCS - Distributed Control System	Systems which control, monitor, and manage industrial processes that are dispersed but operated as a coupled system	Thermal plant auxiliary systems
PCS – Process Control System	Systems which control, monitor, and manage an industrial processes	Thermal power plant, Nuclear Power Plant Systems, Wind Farm, etc.
Building Automation	Control systems used to manage security, safety, fire, water, air handling in a building or facility	Data center’s environmental systems, control centers, etc.
I&C - Instrumentation & Control	Electronic devices or assemblies used to monitor, measure, manage or operate equipment in many applications	Nuclear Power Production
SIS - Safety Instrumented System	System with the sole function to monitor specific conditions and act to maintain safety of the process	Power Plant

**Figure 1.2.** Examples of Electric Power OT

Addressing this issue requires a greater understanding of the work to be performed and the associated competencies to include the necessary knowledge, skills, and abilities required by various job roles. Greater clarity will allow workforce managers, training organizations, educators, and community practitioners to develop programs to supply or to pursue these competencies. Notably, grid modernization efforts must include very advanced and continually maturing cybersecurity capabilities or the power system will not be resilient or reliable (O’Neil et al. 2012).

This project has highlighted the very challenging blend of control engineering and security that is required to protect the OT in smart grid networks and advanced energy control systems. The ability to perform work in these challenging environments often requires a deeper understanding of the work environment and the context of how the technology is implemented and its role in bridging cyber technology to the physical world.

Government and industry now largely agree that the deficit of workers with sufficient cybersecurity expertise is approaching a crisis point as grid complexity increases and the current generation of grid security experts retires (O’Neil et al. 2012). Stakeholders are asking how to collectively accelerate the general maturation of a cybersecurity worker’s knowledge, skills and performance. This question must be expanded to include imparting a special mix of information security, electric power infrastructure, risk, operations, social, analytical and organizational skills to address needs of the power system. The response to this question will illuminate the potential paths to equip properly developed and trained

information security experts with the skills to perform actions that protect grid control systems on infrastructure in a way that is aligned with organizational and regulatory policies and goals. The next step is to identify the resources and mechanisms that are available today and understand their ability to move someone along these paths. Do we need to simply fill in specific gaps to connect the available resources relied upon by the general information security market? Or do we need to develop an additional tier of training to further prepare and qualify cybersecurity professionals to work in electric power system OT applications? These are important questions that should be answered to address the workforce challenges faced by today's electric power system stakeholders. This report begins a process to address these important questions.

An aging workforce presents another critical challenge. A general demographic shift has been impacting well-established industries, resulting in larger than normal turnovers as a population bubble reaches retirement age. The North American Electric Reliability Council's Long-Term Reliability Assessment Report (NERC 2012a) noted that the potential loss of experienced personnel as industry's workforce ages poses a long-term threat to bulk system reliability. There is a unique opportunity and danger as utilities develop programs to replace large numbers of highly experienced staff.

The opportunity comes in turning to younger generations that have extensive experience in computer technology as a part of performing most types of work. However, time is of the essence in preparing this workforce to address the dynamic and rapidly growing cybersecurity threat. A holistic approach to development is needed to accelerate competence development by adapting workforce programs to individual differences in background knowledge, learning styles, and aptitude of workforce entrants (Assante and Tobey 2011; Gandhi et al.<sup>1</sup>). "Holistic" in this context means

- addressing all human factors of accelerated expertise development ("book knowledge," hands-on skills, innate abilities, cognitive/behavioral influences)
- including all phases of the workforce development cycle (assessment, training, certification, retesting, professional development, communities of practice, etc.).

Essentially, holistic development requires a high level of integration among workforce programs to minimize unnecessary duplication or inconsistency that may retard development due to a need to address conflicting priorities.

## 1.2 Study Purpose and Contribution

The U.S. Department of Energy recognized that the electric power industry needs workforce development resources that can make up for the accelerating loss of existing workforce professional, while at the same time building substantial new cybersecurity expertise to protect and enable the modernized grid currently being built. Accordingly, in the spring of 2011 a project was initiated by Pacific Northwest National Laboratory (PNNL) to identify and understand the competencies necessary to perform cybersecurity functions and to assess the need to develop a set of guidelines for a certification program for future power system cybersecurity specialists. The initial scope was the operational security functions for day-to-day operations (but not development, engineering, and architecture) and power system environments. The project examined the technical, problem-solving, social and analytical skills

---

<sup>1</sup> Gandhi RA, DH Tobey, R Reiter-Palmon, M Yankelevich, and K Pabst. 2013. *ADAPTS: An evidence-based cyberlearning network for accelerating proficiency*. Working paper, Omaha, NE.

used by existing cybersecurity staff in the daily execution of their responsibilities. The primary purpose is to answer the questions posed by stakeholders and to develop a model to aid in the development of the necessary technical and operational cybersecurity knowledge, skills, and abilities to achieve modernization goals.

The second phase of this project identified existing frameworks, training courses, and certification programs that may contribute to developing the necessary knowledge, skills, and abilities required of this special workforce. The purpose of this phase was to assess the level of integration among these frameworks, training courses, and certification programs: 1) the degree to which workforce programs emphasize common responsibility areas determined to be critical or differentiating of job performance; 2) the degree to which essential responsibility areas are, or are not, adequately emphasized by these programs; and 3) similar to findings in systems engineering, the degree to which essential responsibility areas may be omitted from current workforce programs. Collectively, these insights will help to guide development and implementation of assessment, certification, education and training program improvements to support the prevention of, or effective response to, cybersecurity vulnerabilities or intrusions within the nation's power systems.

Many of the existing cybersecurity training and certification programs are focused on the general application of cybersecurity and do not provide learning that aligns with some of the unique aspects of performing work in an OT environment. Also, many of the available resources are predicated on testing the "book learning" of security professionals who often study preparation guides before taking the certification exams. The applicability of general resources can be diminished by not providing learning nor measuring/certifying competence in industrial contexts or under real-world conditions where multidisciplinary problem solving and social and intuitive analytical skills are used by security professionals in the daily battle to secure infrastructure technology. Workforce development programs targeting the cybersecurity profession are slowly moving beyond simple knowledge-recall tests of competence. They have begun to measure how knowledge is applied and further, how decisions are made. We must accelerate these efforts and strive to match the rate at which technology is deployed and incorporates the latest vulnerabilities and attack patterns (Wu et al. 2011).

Our exploration of available resources mapped to the responsibilities identified in Phase 1 of this study resulted in specific questions that need to be asked and answered by electric power industry stakeholders. These questions illuminate the need to establish fundamental requirements that will help shape the market and broader ecosystem response and provide better-aligned resources while establishing direction for individual professionals. The challenge can be divided into two broad categories: developing cybersecurity professionals capable of performing work in electric power system OT environments, and augmenting power system operators and engineers with necessary cybersecurity knowledge and skill to do their job and team with cybersecurity professionals. The questions asked by our panel of volunteer subject matter experts (SMEs), after reviewing the results of simple mapping exercises, resulted in the identification of five major research challenges, providing a starting point for a comprehensive effort to develop a cybersecurity informed and competent workforce:

1. What competencies do we need to measure in both electric power system cybersecurity functional job roles and electric power system operations and engineering? What domains of knowledge and types of cybersecurity-associated skills and abilities are necessary for engineers involved in planning and designing industrial systems and the operational technology necessary to support them?

- What domains of knowledge and types of cybersecurity-associated skills and abilities are necessary for engineers involved in operating industrial processes to achieve safe and reliable operating goals?
  - How do various engineering job roles and cybersecurity specialty roles engage to maximize constructive overlap and differences to address security for these systems?
2. How should we conduct tests so they are holistic and accurate, differentiating between simple understanding of concepts and skilled performance of actions that effectively resolve problems quickly and despite distractions or the stress surrounding an attack? (Assessment gap)
  3. How do we prepare professionals for the tests and the real world? (Training gap)
  4. What is the best framework for general cybersecurity certifications that integrate both knowledge and skill while predicting constraints of innate abilities on performance, and do we need OT- or industry-specific certifications? (Certification gap)
  5. How do we support the certified cybersecurity professional and cyber-informed operations and engineering professionals with advanced problem-solving tools, communities of practice, canonical knowledge bases, and other performance support tools? (Support gap)

Even with acknowledgement that the power system is being transformed by technology, many have struggled with how to apply this new reality to traditional job roles and functions. There is an important intersection between the work to secure power systems and the need to operate and manage them in a secure manner and, more importantly, how to respond to security events where the integrity of the system was compromised. This intersection deserves focused inspection and needs to shape our workforce development efforts. Our goal cannot be to make power engineers cybersecurity professionals, but to identify what a System Operator needs to know and apply to their job responsibilities, while sharply defining how these roles interact with those of cybersecurity professionals to achieve greater levels of system reliability. The difficulty in responding to the cybersecurity realities imposed on system operations is best summarized by the North American Electric Reliability Corporation (NERC) High Impact Low Frequency report in 2009, where industry experts explained why grid operators have not traditionally been involved in modifying their work practices to address cyber events: “As a coordinated attack has not been experienced to date, an operator faced with such an attack would have no real-life experience to draw on when responding to it. Further, little training presently exists to drill responses to these events, though certain organizations have recently begun to incorporate this material into their training programs (NERC 2010, pg 33).” The High Impact Low Frequency report goes on to propose action: “NERC’s Board of Trustees should direct its committees to support and promote the development of System Operator training scenarios for physical and cyber attack. The group should consider recommendations to NERC’s System Operator Certification and Continuing Education Program for potential training requirements (NERC 2010, pg 41).”

Industry has not ignored this specific challenge. A more focused investigation by industry practitioners participating in the NERC Cyber Attack Task Force (CATF) concludes,

Training needs to include not only operators but field technicians as well. Focus should be on establishing a baseline to judge if “something looks or acts differently.” Then, the training needs to exercise the entities incident response plan which includes reporting (NERC 2012b, pg 20).

This study attempts to inform the exploration of this challenge and attempts to identify whether existing resources exist to deliver the type of training that is required. It provides the results of the second phase of the three-phase study being conducted for the U.S. Department of Energy through a partnership of PNNL and the National Board of Information Security Examiners (NBISE) to produce and apply a comprehensive Job Performance Model (JPM) for Smart Grid Cybersecurity developed during the first phase of the project (O’Neil et al. 2012). A JPM is a list of competencies, often organized into five or more groupings or clusters, attributable to satisfactory or exceptional employee performance for a specific job role.

The first phase produced an exploratory JPM based on a factor analysis of responses to a Job Analysis Questionnaire. The result was an initial Smart Grid Cybersecurity Job Performance Model, for selected cyber roles, that detailed the fundamental and differentiating competencies necessary to successfully protect and defend power systems from cybersecurity attack. During this phase, critical incidents (Flanagan 1954; Klein et al. 1989) captured as a series of vignettes, or deconstructed stories (Boje 2001; Tobey 2007) of a significant or potentially significant cybersecurity event were transformed into a detailed list of goals, objectives, responsibilities, and tasks for the functional and job roles involved in smart grid cybersecurity.

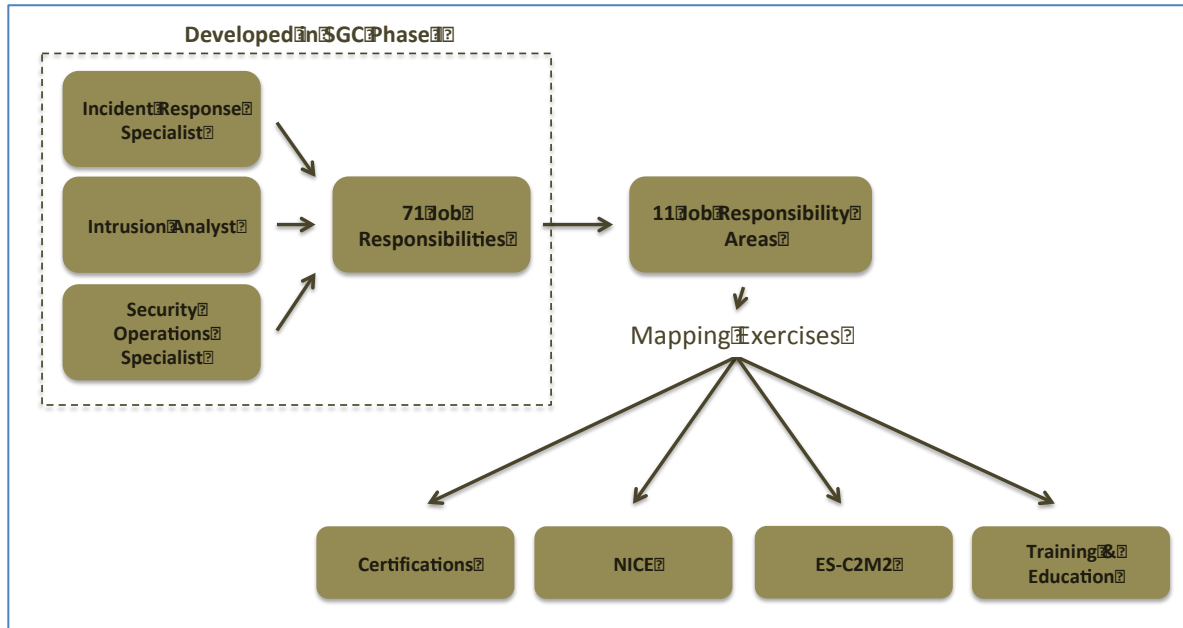
“I believe these results confirm a common belief within [power and utility] entities that; traditional IT roles are fairly well defined with credentials and available credentials, while Operations Technology roles do not have a well-defined alignment to existing [cybersecurity] programs.”  
- **Tim Conway**, Panel Chair

#### NERC CATF Report recommendations for power system entities

- **Continue to Develop Security and Operations Staff Skills to Address Increasingly Sophisticated Cyber Threats** – Entities should develop strategies to attract cybersecurity talent and further develop the knowledge, skills, and abilities of existing staff to address increasingly sophisticated cyber threats and technology challenges that accompany grid modernization efforts.
- **Augment Operator Training with Cyber Attack Scenarios** – Several cyber attack scenario templates are included in Appendix C of this report. Entities should consider enhancing training to incorporate cyber attacks that raise operator awareness for a coordinated cyber attack.
- **Conservative Operations** – The *Severe Impact Resilience: Considerations and Recommendations* report prepared by the Severe Impact Resilience Task Force offers a number of recommendations regarding conservative operations. Entities should review this report and consider the practices that would apply to a coordinated cyber attack scenario.

The second phase of the project applied the JPM to ascertain the alignment and gaps among existing workforce development programs. The JPM included three job roles for which 82 job responsibilities were identified; 71 of these job responsibilities were assigned by the SME panel in this second phase to 11 job responsibility areas. The remaining 11 responsibilities were not considered by the SME panel to be sufficiently related to one or more of the identified areas for the target job roles, nor related to each other sufficiently to create an additional responsibility area. They were therefore removed for further consideration by the panel, but are reserved for future use as they may be related to other job roles. These responsibility areas became the basis for studying the gaps and overlaps between four cybersecurity

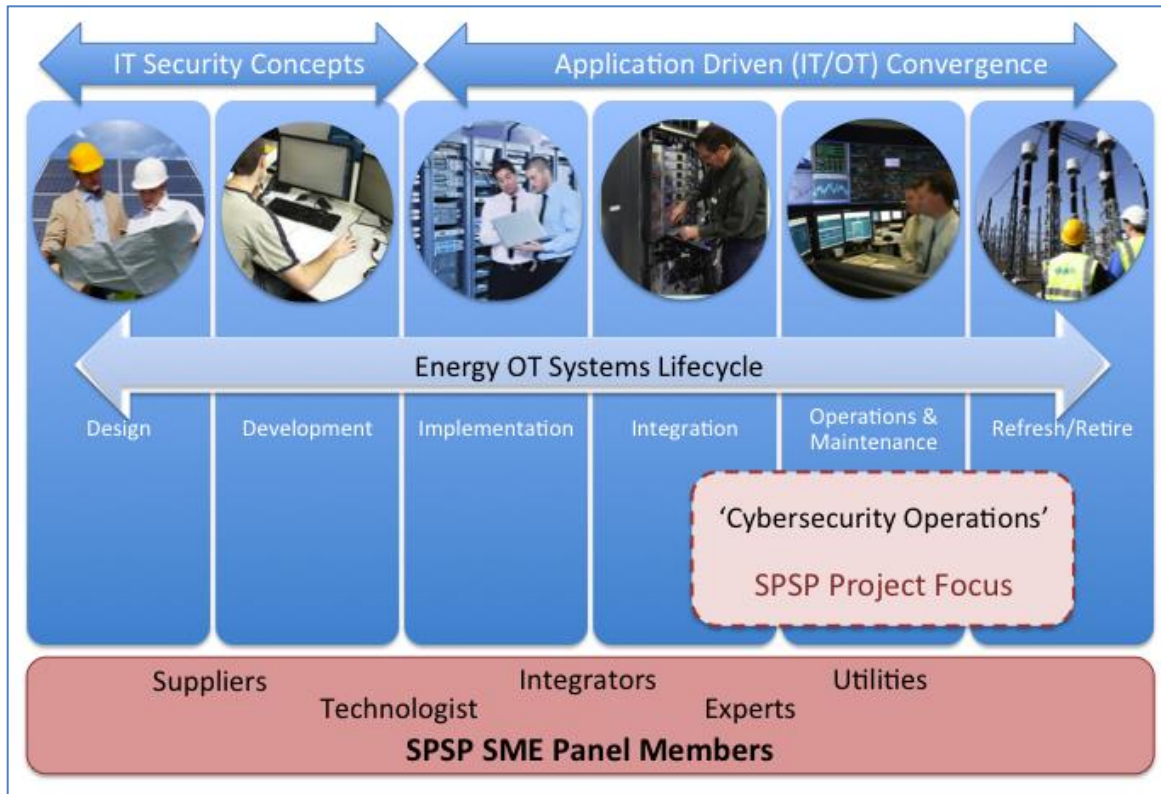
workforce development programs: 1) the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework; 2) the Energy Systems Cybersecurity Capability Maturity Model (ES-C2M2); 3) power systems cybersecurity education courses; and 4) cybersecurity certifications (see Figure 1.3). The panel's findings were then reviewed through a public survey. The results of the SME panel analysis and the public survey suggest responsibility areas lacking any or sufficient coverage in the current workforce programs, or areas where a lack of consensus suggests further analysis is needed. Overall, the results of the study provide insights into requirements for adjustment, application, or enhancement of these four workforce programs to improve decision-making on identification, assessment, and development of power systems cybersecurity talent.



**Figure 1.3.** Phase 2 Mappings

The gathering, analysis, and mapping of cybersecurity workforce development resources raise important questions about the integration and combinations of responsibilities for cyber specialists and the engineers responsible for the design and operations of OT. Existing resources appear to make few distinctions, treating general cybersecurity the same across security, information technology, and engineering disciplines with some depth toward cybersecurity specialties. In an age of specialization, one of the primary issues has to do with how much general knowledge or skill is necessary for one job role compared to another. Another concern is the identification of overlap and differentiation among job roles, as necessary. Cybersecurity staff task execution-sequencing matters. A high level of coordination is required to be successful at detecting and responding properly to cyber events in industrial control systems (ICS).

Cybersecurity operations involve a myriad of concepts and systems across information security and operational technology disciplines. Figure 1.4 depicts an energy OT systems life cycle and reflects the focus areas of the Secure Power Systems Professional Project. Cybersecurity staff often become involved with job tasks that pertain to information security and operations technology staff. Accordingly, the Secure Power Systems Professional SME panel included information security and operations technology experts.



**Figure 1.4.** Energy OT Systems Lifecycle

The challenges identified require action from a diverse set of stakeholders (this includes individual electric power entities, the electric power industry, power system suppliers, integrators, researchers, educators, and training organizations). This report aims to provide data and SME observations and discussions to help inform additional discussion and action. There are a myriad of focus areas that will contribute to progress. Many of them can begin with sharing information and articulating the needs of various stakeholders. Some examples of relevant discussions and information sharing include

- publishing workforce requirements and identifying of specific cybersecurity competencies and the unique demands required to apply them to power systems
- considering the value of developing a focused OT (SCADA/ICS-specific) cybersecurity certification that can support ICS-reliant industries
  - considering what knowledge may be valuable to power system operations and engineering staff as identified in past industry studies
- encouraging the development of cyber curriculum elements for power engineering educational programs
  - understanding the implications of human-centric cyber risks to system reliability
  - defining what “cyber-informed engineering” means and how considering cyber risks can improve system design, planning, and operations.



The final phase of the project will involve analyzing data generated from Phase I and Phase II to provide guidelines for implementing an assessment program to help organizations and individuals better plan and protect power systems from cybersecurity attacks by using predictive, analytical techniques for talent management (Boudreau and Ramstad 2005). Additionally, this final report will identify future research and practice implications for development of training modules and simulation practice environments that may be used to accelerate proficiency in smart grid cybersecurity jobs.

### **1.3 Previous Work in Competency Models and Workforce Development**

Competency models, capability maturity models, course learning objectives and topics, and certification objectives and requirements should ideally be well aligned to facilitate a holistic approach to workforce development (Assante and Tobey 2011). Over the past several years, national initiatives have formed to create a Common Body of Knowledge (Bishop and Engle 2006; Theoharidou and Gritzalis 2007) or criteria for achieving excellence in information assurance education (Schweitzer et al. 2006). Similar efforts in the related field of systems engineering have found that competing and often incomparable competence frameworks develop because they lack a common, validated, predictive model of job performance that facilitates alignment among aptitude and achievement assessments, curriculum designs, and performance evaluation systems (Towhidnejad et al. 2013). Kasser et al. (2012) recently analyzed nine such workforce programs for systems engineering. The authors found that while each workforce program provided useful guidance, they emphasized different responsibility areas, which made it difficult to compare and integrate the models into a holistic workforce development program. Furthermore, Kasser et al. found that definitions of required knowledge, skill and abilities lacked an organized and comprehensive structure. Finally, and perhaps most important, these nine frameworks omitted fundamental job responsibilities that were critical for effective job performance. The study authors concluded (Kasser et al. 2012, p. 40):

“... competency models may suffer from errors of omission because the development methodology does not include a validation function to determine if something that should be done is not being done (and the effect of that lack may not show up for some months or even years). Indeed, this research has identified an error of omission in all of the nine competency models studied, namely, the lack of competencies in the implementation domain.”

Implementation is a primary concern for cybersecurity workforce programs. The CSIS (Center for Strategic and International Studies) Commission on Cybersecurity for the 44<sup>th</sup> Presidency was established to identify the requirements for effective response to the increasing threat of cybersecurity attacks. The Commission concluded, “We not only have a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate, and reconstitute from damage due to system failures and malicious acts” (CSIS 2010, pg 2). This 2010 CSIS Commission report, *A Human Capital Crisis in Cybersecurity - Technical Proficiency Matters*, outlines elements that a successful strategy must include the following:

- Promote and fund the development of more rigorous curricula in our schools.



- Support the development and adoption of technically rigorous professional certifications that include a tough educational and monitored practical component.
- Use a combination of the hiring process, the acquisition process and training resources to raise the level of technical competence of those who build, operate, and defend governmental systems.

The CSIS Commission report recognizes that developing a “pivotal talent pool” (Boudreau and Ramstad 2005) requires the implementation of integrated competency models, educational curricula, certifications, and maturity models which indicate an increased level of technical competence in the workforce.



## **2.0 Method**

### **2.1 Panel Composition**

The initial pool of panel members (32 male, 1 female) for this project phase included 33 SMEs (see Appendix A for a complete roster). The panel was advised and facilitated by the NBISE and PNNL project team (3 male, 3 female). The initial panel was formed with members from the power industry (26.5%), technology vendors (23.5%), professional services firms (23.5%), government agencies (11.8%), and research organizations (11.8%). The selection of panelists was based on their expertise in the relevant fields, availability of sufficient time to commit to the project, and maintaining a diverse representation of the interested stakeholders. The panelists were also widely distributed geographically.

### **2.2 Panel Activities**

Panel members participated in four sessions over a five-and-a-half month period. The first three sessions were focused on eliciting information and rating responses in order to derive a mapping of responsibility areas from the Smart Grid Cybersecurity Job Performance Model developed in Phase 1 (SGC-JPM; O’Neil et al. 2012) to each of four workforce development programs that were the focus of analysis in this project phase: certification domains, NICE Tasks, ES-C2M2 objectives, and education course topics (hereafter referred to as “target workforce programs”). Each session was scheduled for more than one time slot, and allowed for asynchronous participation to accommodate member’s scheduling constraints. The first session was held on October 31, 2012, and the last was held on April 16, 2013. The activities, participation rates, and methodology for each session are provided in Appendix B. Participation of the panel in the sessions ranged from 6 to 23 members with a mean participation per session of 16 members (46%) from the SME pool per session.

Three studies were conducted during this phase. First, the SME panel was asked to analyze the value, commonality, and mapping of certification exams to power system cybersecurity job role responsibilities. The purpose of this first study was to determine whether the SGC-JPM created in the first phase of the project added value in identification of gaps and overlaps in applicable certification programs. This pilot study showed that the JPM provides sufficient detail to derive insights about the gaps, overlaps and maturity of workforce programs. After a minor change in the way the job responsibilities were presented, a similar analysis was performed on the remaining three workforce programs. Finally, a survey was created to obtain public review and comment on the results obtained from the first two studies.

### **2.3 Review and Comment System**

The public survey was developed based on the analysis of the panel responses to obtain feedback and seek verification of the panel findings regarding the alignment of workforce programs with the job responsibilities. An email was sent through a variety of channels requesting participation from individuals with experience in power systems cybersecurity. After clicking on the survey link in the email, a respondent would be taken to a landing page where instructions were provided for completion of a demographics questionnaire, followed by their choice of completion of up to four workforce program questionnaire pages (see Appendix K for the instructions and a sample questionnaire page). The

instructions emphasized that individuals should only complete questionnaires for workforce programs if they felt that they had sufficient expertise.

A total of 127 people (113 male, 13 female, 1 unreported) accessed the landing page and completed a demographic survey. Forty-one respondents (35 male, 5 female) elected to complete one or more workforce program questionnaires, with an average of 2.6 questionnaires completed per respondent. Demographic details of the respondents to the workforce program questionnaires may be found in Appendix D. A chi-square test found that the respondents completing the workforce program questionnaires did not differ from those who only completed the demographic survey in terms of age ( $p = 0.54$ ), years of experience ( $p = 0.23$ ), or job title ( $p = 0.68$ ). However, a marginal difference was found in terms of expertise levels ( $p = 0.08$ ), but this difference was in the expected direction. None of the individuals reporting their expertise as a novice completed a workforce program questionnaire, and only 2.4% of those completing these questionnaires listed their expertise as a beginner, while 12.8% has done so in the demographic survey. In summary, 97.6% of those completing the workforce questionnaires indicated their expertise level was proficient or better, consistent with the request that only those qualified to perform cybersecurity-related jobs provide responses to the workforce program questionnaires.

## **2.4 Agreement Analyses**

Inter-rater agreement analyses were conducted for each activity involving panel or public rating of items. The Fleiss' Kappa measure (Fleiss and Cuzick 1979; Fleiss 1971) was used to determine the level of agreement for activities involving the assignment of items within a single category, e.g., certification domains applicable to job roles. The Fleiss' Kappa measure varies from just under 0 to 1, with larger values meaning more agreement. The p-value is the statistical probability of the null hypothesis ("No Agreement" or Fleiss' Kappa = 0) being true. In this case, p-values above 0.01 (alpha) were viewed as not rejecting the null ("No Agreement"), and p-values less than 0.01 were viewed as being in some degree of agreement (statistically speaking). Agreement among panel and public ratings of the relative emphasis provided by the target workforce programs to the responsibility areas from the SGC-JPM were evaluated using the G-index developed by Holley and colleagues (Holley and Guilford 1964; Holley and Lienert 1974). This index was developed to evaluate agreement among multiple raters placing items into multiple categories. According to Landis and Koch (Landis and Koch 1977), a G-index of greater than 0.6 is associated with substantial agreement, a G-index value between 0.2 and 0.6 denotes fair to moderate agreement, and a G-index below 0.2 denotes poor agreement.

Panel responses showed agreement in determining the importance of specific certifications for assessing competence in each of four job roles that were the focus of this phase of the project: Intrusion Analysis; Security Operations; Incident Response; and Cyber Secure Power Engineer. Panel responses also showed agreement in assignment of job responsibilities to the job roles of Intrusion Analysis and Incident Response. The panel lacked agreement in assigning job responsibilities to security operations and the cyber-secure power engineer job roles. Further details on the results of the inter-rater agreement analysis for these activities may be found in Appendix F. Agreement among panel and public responses for the mapping of responsibility areas to the target workforce programs is discussed in the Findings section below.

### 3.0 Findings

The first activity for the SME panel was to rate the importance of certifications for assessing competence in the target job roles. Sixty-four certifications were presented to each panel respondent (see Appendix C). For each certification, the respondent indicated whether they thought the certification was common or uncommon for incumbent professionals in power system cybersecurity job roles, and whether such certification was valuable for assessing competence. This analysis yielded ten vendor-neutral certifications (listed in Figure 3.1) that most panel members indicated were valuable for determining job competence.

<b>Certification</b>	<b>Organization</b>
Certified Information Systems Security Professional (CISSP)	(ISC) <sup>2</sup>
System Operator Certification (SOC)	NERC
Certified Ethical Hacker (CEH)	EC-Council
Certified information Security Auditor (CISA)	ISACA
Certified Information Security Manager (CISM)	ISACA
Certified in Risk and Information Systems Control (CRISC)	ISACA
Certified Incident Handler (GCIH)	GIAC
Certified Intrusion Analyst (GCIA)	GIAC
Penetration Tester (GPEN)	GIAC
Web Application Penetration Tester (GWAPT)	GIAC

**Figure 3.1.** Valuable Vendor-Neutral Certifications

Each of the certifications that were deemed valuable was further classified by the panel into knowledge domains based on the learning objectives of the certification. Appendix G provides a comparative matrix of these certifications, documenting the domains/attributes/skills that each certifies. The SME panel rated the relevance of each certification for the job roles that were the subject of the first phase of this project: Security Operations, Intrusion Analysis, and Incident Response. Additionally, we examined the relevance of these certifications in a general functional role of Cyber Secure Power Engineer. The results of the job role analysis are provided in Table 3.1.

**Table 3.1.** Vendor-Neutral Certifications Related to Job Roles

Target Job Role	Certifications	Certifying Organization
Cyber Secure Power Engineer	Certified Information Systems Security Professional (CISSP)	(ISC) <sup>2</sup>
	System Operator Certification (SOC)	NERC
Incident Response	GIAC Certified Incident Handler (GCIH)	GIAC
	Certified Information Systems Security Professional (CISSP)	(ISC) <sup>2</sup>
	Certified Hacking Forensic Investigator (CHFI)	EC-Council
	GIAC Certified Forensic Analyst (GCFA)	GIAC
	GIAC Certified Intrusion Analyst (GCIA)	GIAC
	GIAC Certified Windows Security Administrator (GCWN)	GIAC
Intrusion Analysis	GIAC Certified Intrusion Analyst (GCIA)	GIAC
	Certified Ethical Hacker (CEH)	EC-Council
	Certified Information Systems Security Professional (CISSP)	(ISC) <sup>2</sup>
	GIAC Certified Forensic Analyst (GCFA)	GIAC
	GIAC Penetration Tester (GPEN)	GIAC
	Certified Hacking Forensic Investigator (CHFI)	EC-Council
	GIAC Certified Forensic Examiner (GCFE)	GIAC
	GIAC Reverse Engineering Malware (GREM)	GIAC
	Security Certified Network Professional (SCNP)	SCP
Security Operations	Certified Information Systems Security Professional (CISSP)	(ISC) <sup>2</sup>
	Certified Information Security Manager (CISM)	ISACA
	GIAC Security Essentials (GSEC)	GIAC
	GIAC Certified Enterprise Defender (GCED)	GIAC
	GIAC Security Leadership (GSLC)	GIAC
	Certified Ethical Hacker (CEH)	EC-Council
	GIAC Certified Firewall Analyst (GCFW)	GIAC
	GIAC Information Security Fundamentals (GISF)	GIAC
	GIAC Information Security Professional (GISP)	GIAC
	System Operator Certification (SOC)	NERC
EC-Council = International Council of Electronic Commerce Consultants GIAC = Global Information Assurance Certification ISACA = Information Systems Audit and Control Association ISC = Industrial Control Systems NERC = North American Electric Reliability Corporation		

Appendices E through J provide the detailed results from the SME panel votes mapping the certification exams, the two competency model frameworks (NICE and ES-C2M2), and the course topics to responsibilities. Below we will briefly summarize the findings in each competency indicator category.

### 3.1 Certifications Mapped to Job Responsibilities

Responsibilities were assigned by the panel to the four job roles analyzed during this phase of the project. Appendix L lists the votes of the panel assigning responsibilities to each role. Each responsibility was then mapped by the panel to the set of learning objectives from certifications related to that job role. Each certification differs in the degree of detail provided for that certification's learning objectives. Consequently, the number of learning objectives that could be mapped between a certification and a specific job role will markedly differ. Therefore, a simple comparison of the number of responsibilities mapped to a certification is not a good indicator of the breadth of coverage for a particular

responsibility. Accordingly, this analysis focused on the number of responsibility areas each certification covers with a minimum match—at least one learning objective had to be assigned to a responsibility. Table 3.2 shows the results of this analysis for each job role by listing the certifications that are associated with a job role, the number of responsibilities addressed by that certification, and the percentage of the total number of responsibilities for that job role addressed by the certification. The table also shows the number of responsibilities not associated with any of the included certifications. For detailed results and a description of the inter-rater agreement results see Appendices I and F.

**Table 3.2.** Certifications Associated with Job Roles

Job Roles	Certifications	# of Resp.	% of Resp.
Cyber secure power engineer (9 responsibilities)	CISSP	3	33.3%
	CISM	1	11.1%
	Not covered by certification	6	66.7%
Incident response (10 responsibilities)	CISM	4	40.0%
	CISSP	3	30.0%
	GCIH	9	90.0%
	Not covered by certification	0	0.0%
Intrusion analysis (10 responsibilities)	CISM	3	30.0%
	CISSP	2	20.0%
	GCIH	7	70.0%
	CEH	1	10.0%
	GCIA	1	10.0%
	Not covered by certification	2	20.0%
Security operations (16 responsibilities)	CISM	8	50.0%
	CISSP	7	43.8%
	GCIH	3	18.8%
	Not covered by certification	5	31.3%
CEH = Certified Ethical Hacker			
CISM = Certified Information Security Manager			
CISSP = Certified Information Systems Security Professional			
GCIA = Certified Intrusion Analyst			
GCIH = Certified Incident Handler			

### 3.1.1 Discussion of Certification Review Results

The results of the certification review indicate that no single certification can be relied upon to adequately test knowledge necessary to perform the responsibilities for each of the target job roles. Table 3.3 shows the percentage of responsibilities covered by six certifications as an example of how responsibility mapping facilitates comparison of certification programs. A responsibility may be covered by more than one certification and may be assigned to more than one job role, so the rows and columns may exceed 100%. Accordingly, the table provides an indication of the relative emphasis that a certification may place on a respective role (by analyzing a column), or the relative emphasis that should be placed on a certification when determining achieved proficiency in a job role (by analyzing the rows). Finally, the table demonstrates where gaps and overlaps may exist. For example, as noted above, the Cyber Secure Power Engineer role has not received sufficient coverage in current certifications. Furthermore, despite being considered a valuable certification, the System Operator Certification (SOC),

does not currently cover any of the cybersecurity responsibilities identified for the four job roles. Overall, the CISSP appears to offer the broadest and most balanced coverage of all the certifications followed by the CISM. GCIH appears to be a specialist certification, while the CEH, GCIA, and SOC certifications were not found to measure knowledge for a significant number of responsibilities assigned to the target job roles.

**Table 3.3.** Job Role Coverage by Certification

Job Role	CEH	CISM	CISSP	GCIA	GCIH	SOC
Cyber Secure Power Engineer	0.0%	11.1%	33.3%	0.0%	0.0%	0.0%
Incident Response	0.0%	40.0%	20.0%	0.0%	90.0%	0.0%
Intrusion Analysis	10.0%	30.0%	20.0%	10.0%	70.0%	0.0%
Security Operations	0.0%	50.0%	37.5%	0.0%	18.8%	0.0%
CEH = Certified Ethical Hacker CISM = Certified Information Security Manager CISSP = Certified Information Systems Security Professional GCIA = Certified Intrusion Analyst GCIH = Certified Incident Handler SOC = System Operator Certification						

This review of certification learning objectives suggests that cybersecurity job roles differ in the level of maturity. Some roles, such as Incident Response, appear to have at least a minimal level of coverage of each job responsibility in certification exams. This traditional cybersecurity role represents one extreme. At the other extreme is the newly identified role of Cyber Secure Power Engineer. In this case, few of the certifications addressed the specific responsibilities to be fulfilled by this job role. Accordingly, existing certification exams include few learning objectives mapped to the responsibilities of these four job roles. The remaining two job roles studied in this phase, Intrusion Analysis and Security Operations, are arrayed between these extremes. Intrusion Analysis appears to be more mature with 80% of the responsibilities covered by certification exams. Security Operations shows a lack of consensus over the job definition and less alignment with existing certification exams, with roughly two-thirds coverage of job responsibilities.

In summary, the results of this first panel activity suggest that by delineating specific responsibilities for each job role, the SGC-JPM enabled identification of potential alignment and gaps in a workforce development program—certification exams. However, the overlap among responsibilities at both the certification and job role levels suggested that a set of mutually exclusive responsibility areas might provide greater clarity for comparing and contrasting workforce programs. Notwithstanding this limitation of the first study, the results showed considerable variance in the degree to which the SME panel concurred on the breadth of responsibilities for each job role, and accordingly the degree to which these responsibilities were included in certification exams.

These results support recent efforts to better define cybersecurity roles and develop assessments of their maturation (Moore and White 2012; NIST 2011; Paulsen et al. 2012). Further, these results suggest that such competency frameworks must provide detailed responsibility and task lists. Otherwise, alignment may be difficult to achieve with other workforce programs, such as education or certification. To analyze the degree to which such alignment exists, in the next set of activities the SME panel evaluated two competency frameworks—the NICE and the ES-C2M2—and a collection of syllabi for educational programs intended to develop proficiency in the four job roles.



### 3.2 Competency Frameworks and Course Topics

To address the limitation of the first study, and to facilitate comparative analysis of multiple workforce programs, the 71 job responsibilities were categorized into mutually exclusive responsibility areas (see Figure 3.2). The result was a list of eleven responsibility areas that would be used throughout the remaining SME panel activities to compare and contrast the two competency frameworks (NICE and ES-C2M2) and the two workforce development programs (education courses and certifications). Using open source research the project team identified 32 courses that focus on cybersecurity and OT; eight of these courses were not included as we were unable to obtain objectives for these courses, which are required for the analysis (see Appendix M for a list of courses). These courses were organized more toward topic areas rather than job roles. The courses were mostly industry agnostic, but some did contain work examples and knowledge that can be applied in the electric power industry. Table 3.4 summarizes the findings regarding the SME panel mapping of the eleven responsibility areas to the competency frameworks and course topics.<sup>1</sup> Appendix J provides a detailed list of the NICE Tasks, ES-C2M2 objectives, and course topics that were identified for each responsibility area.

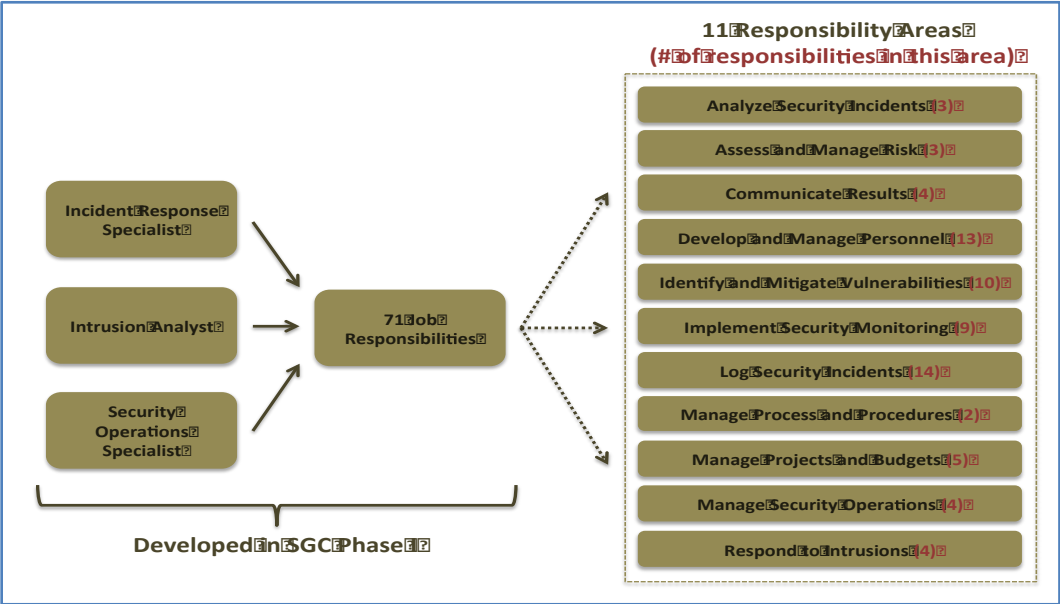


Figure 3.2. Mapping to Responsibility Areas

<sup>1</sup>Workforce frameworks refer to cybersecurity role descriptions and organizational staffing references. Course topics are publicly provided descriptions of a cybersecurity course’s learning objectives or an outline and curriculum description.

**Table 3.4.** Coverage of Responsibility Areas in the Competency Frameworks and Course Topics

Responsibility Area <sup>(a)</sup>	NICE Tasks	ES- C2M2 Objective	Course Topics
Analyze security incidents	14	2	2
Assess and manage risk	9	4	9
Respond to intrusions	10	3	1
Communicate results	11	3	0
Identify and mitigate vulnerabilities	11	2	11
Implement security monitoring	2	1	6
Log security incidents	6	2	3
Manage process and procedures	3	8	2
Manage projects and budgets	1	1	0
Manage security operations	3	8	5
Develop and manage personnel	0	4	1

ES-C2M2 = Energy Systems Cybersecurity Capability Maturity Model  
NICE = National Initiative for Cybersecurity Education  
(a) Technical responsibilities are shaded in blue; managerial responsibilities are shaded in gray.

### 3.2.1 Discussion of Responsibility Area Mappings

The current workforce development frameworks and education programs appear to be focused on very different aspects of the cybersecurity function. Table 3.4 shows each of the responsibility areas along with the number of competency indicator items that were mapped to it. Most notable in this table is the relative difference in emphasis of competency indicators focused in each responsibility area across the two competency model frameworks and course topics.

First, the responses from the SME panel suggest that technical responsibilities are a significant focus of the NICE task list and the education and training course topics (blue area at the top of Table 3.4) while the ES-C2M2 provides the greatest weighting to individual responsibility areas that reflect a managerial focus (gray area at the bottom of Table 3.4). The NICE task lists provide the most weight to analyzing security incidents while the course topics provide the most emphasis on identifying and mitigating vulnerabilities. Interestingly, while the NICE Framework emphasizes incident analysis, communicating results, and responding to intrusions, the courses examined provide little to no coverage in these areas. Additionally, no emphasis was provided in either the NICE task list or in cybersecurity course topics to developing and managing personnel.

## 3.3 Combined Panel and Public Responsibility Area Mappings

Figure 3.3 shows the combined results of the SME panel and public questionnaire respondent mapping of job responsibility areas to workforce programs. There were six responsibility area mappings (13.6%) of the 44 possible where the results from the public review differed from the results obtained from the SME panel members. The six areas of disagreement between the SME panel members and the public survey respondents are indicated with a “D” in Figure 3.3 (for further detail see Appendix E).

The NICE and the ES-C2M2 are both competency frameworks intended to serve as guides to those developing the other two workforce programs: education and training courses and/or assessment or certification programs. Common emphasis was found in only two areas: assessing and managing risk and communicating results. Both frameworks had limited emphasis on developing and managing personnel, implementing security monitoring, logging security incidents, and managing projects and budgets. The remaining five responsibility areas were emphasized by only one of the competency frameworks.

Similarly, the two workforce development programs (certifications and courses) could be compared and contrasted in terms of the relative emphasis on cybersecurity job responsibilities in their programs. Both workforce development programs were found to emphasize three responsibilities: assess and manage risk, identify and mitigate vulnerabilities, and manage security operations. Four responsibility areas were found to have limited emphasis in workforce development programs: develop and manage personnel, manage process and procedures, manage projects and budgets, and respond to intrusions. The remaining four responsibility areas were emphasized by only one of the workforce development programs.

Responsibility Area	Competency Frameworks		Workforce Development	
	NICE	ES-C2M2	Certs	Courses
Manage projects and budgets				
Develop and manage personnel		D		
Manage process and procedures				
Log security incidents				D
Respond to intrusions				
Implement security monitoring				
Identify and mitigate vulnerabilities			D	
Analyze security incidents				D
Communicate results				
Manage security operations	D		D	
Assess and manage risk				
Shading indicates emphasis on a responsibility area in a competency framework or a workforce development program.				
D indicates mappings with disagreement between panel and public respondents.				
NICE = National Initiative for Cybersecurity Education				
ES-C2M2 = Energy Systems Cybersecurity Capability Maturity Model				

**Figure 3.3.** Target Workforce Program Emphasis of Responsibility Areas

### 3.3.1 Discussion of Public Review and Comment System Results

In general, the public respondents confirmed the results obtained from the SME panel regarding the degree of emphasis given the power system cybersecurity job responsibility areas by each of the four workforce programs. Furthermore, in three of the six area mappings where differences were found between the responses from panel and the public, the panel had showed a lack of consensus among themselves. Thus, it may generally be concluded that responses from the panel and public may be reasonably combined to support stronger observations regarding the relative emphasis and therefore alignment, misalignment, or gaps in coverage among the four workforce programs.

Overall it is somewhat surprising that workforce programs place limited emphasis on the responsibilities targeting the development and management of personnel. It is important to note that these

frameworks are designed to inform the organization and management as to existing and desired capabilities and levels of maturity. Perhaps an excessive focus on the technical responsibilities of these critical jobs has lessened the emphasis on developing or managing the capabilities of the teams they may have reporting to them. Alternatively, the lack of emphasis on personnel development may reflect an assumption that these job roles do not generally have many people directly reporting to them, and hence the lack of emphasis managing and developing staff is warranted. In fact, more than half (53.7%) of those responding to the public survey had no direct reports. This may also explain the relatively limited emphasis on managing projects and budgets, as only 7.3% of the public respondents had more than 30 members of their staff, suggesting that budget and project management responsibilities of these job roles may be in response to managerial and executive directives outside their control. If the responsibilities for managing personnel, projects and budgets are directed by others, then it is reasonable that workforce programs targeting the four cybersecurity job roles studied would not emphasize these responsibilities. However, as the new cybersecurity job roles or function grows in importance, there may be a need to gain the necessary managerial knowledge, skills, and capabilities to oversee the growing cybersecurity professional teams.

Finally, the overall analysis suggests there is much work to be done to align responsibilities that are emphasized by these programs. If managing people and projects are excluded, four of the nine remaining responsibilities (44.4%) are emphasized by either competency frameworks or workforce development programs, but not both. Moreover, seven of the remaining nine responsibility areas (77.8%) are emphasized in one of the competency frameworks, but not the other; six of nine (66.7%) responsibility areas are emphasized in one of the workforce development programs, but not the other. This degree of misalignment may have resulted from emerging cybersecurity challenges outstripping the traditional workforce program's capability to adapt to these challenges, thus requiring a paradigm shift in training/certification approach to meet the current requirements.

### **3.4 Relative Emphasis on Critical and Differentiating Job Responsibilities**

The culmination of the first phase of the project (O'Neil et al. 2012) was the Critical Differentiation Matrix which was used to identify the fundamental and differentiating tasks to be performed by power system cybersecurity staff. We defined fundamental tasks as those that are rated as highly critical to perform, but their execution does not help to differentiate the level of expertise of the performer. Performance on fundamental tasks is essential and should be considered minimal entrance requirements for the field. We defined differentiating tasks as those that are both highly critical and which are performed differently, or substantively different outcomes are produced, by persons with higher levels of expertise than when the task is performed by someone with lower expertise. Differentiating task performance is, therefore, the best indicator of competence. In the final analysis, the Critical Differentiation Matrix value of each responsibility area was used to determine the best application of each workforce program.

Table 3.5 shows a fundamental and differentiating score for each workforce program based on a simple sum of the z-scores for associated responsibility area emphasis.<sup>2</sup> This descriptive analysis limits

---

<sup>2</sup> See (O'Neil, Assante, and Tobey 2012) for an example of how fundamental and differentiating scores are calculated in preparation of a Job Performance Model.

inferences that can be drawn from the data, but suggests that certifications may provide the best guidance for ascertaining fundamental competence in the workforce, while the ES-C2M2 framework may provide the best guidance for ascertaining the competencies that differentiate those individuals (or organizations) with the greatest expertise. These results seem to be well aligned with the respective missions of these programs: certifications establish the baseline for entry into the workforce, and a capability maturity model provides guidance on the relative level of expertise obtained over time. The results also suggest that education courses currently provide strong support for fundamental competencies, but are not addressing the responsibility areas that differentiate those with higher levels of expertise. This may reflect the relatively recent introduction of these courses and/or their target audience may be those who are early in their cybersecurity careers, such as college students, rather than practitioners or graduate students seeking advanced certificates or degrees. Finally, these results suggest that the use of a job performance model as the basis for program comparison, or individual or organizational assessment, has strong face validity—the study results show that the responsibility areas which were found to be emphasized by each program are consistent with that program’s stated mission.

**Table 3.5.** Comparison of Fundamental and Differentiating Emphasis in Workforce Programs

Classification	NICE Framework	ES-C2M2 Framework	Courses	Certifications
Fundamental	6.089	0.344	6.348	9.859
Differentiating	1.249	3.032	−2.426	1.041
ES-C2M2 = Energy Systems Cybersecurity Capability Maturity Model				
NICE = National Initiative for Cybersecurity Education				



## 4.0 General Discussion

### 4.1 Review of Results by Panel Leadership

The studies reported herein involved input from multiple entity perspectives and multiple sectors. Consequently, the results should generalize across a broad range of organizations in the power industry. This study has several implications for determining the competency models, maturity assessments, certifications, and training programs of value for particular job roles. First, entities can immediately use the roles identified to have strong alignment with available certifications of value to adjust job postings or training programs for staff in those roles. Second, for the areas where strong alignment with an existing certification does not exist, entities can first adjust job descriptions and career paths to remove credential requirements that do not align with job-identified roles. Third, organizations can begin developing or working with partners to utilize training programs that best fill the identified gaps. Panel leadership believes these results confirm a common belief within entities that traditional Information Technology (IT) roles are fairly well defined with credentials and available credentials, while OT roles do not have a well-defined alignment to existing programs.<sup>1</sup>

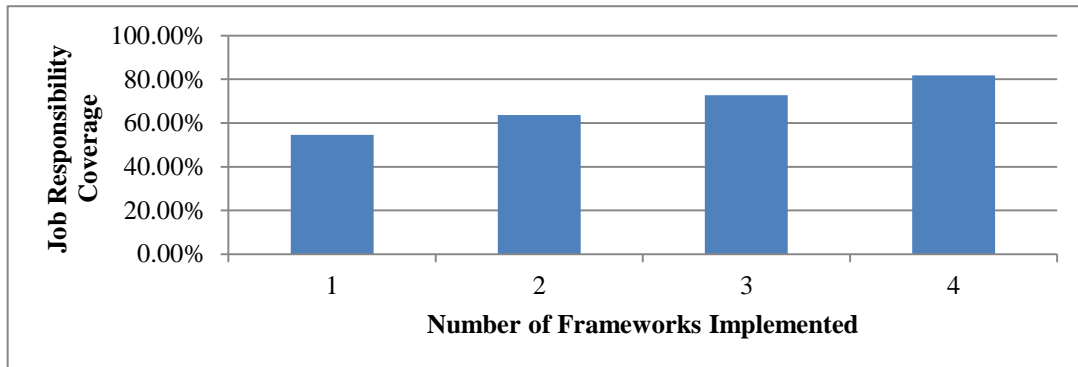
In analyzing the data developed in Phase 2, the panel developed some further findings that help in understanding the implications of these results to electric power industry entities and the cybersecurity workforce. The results of the vendor-neutral certification review indicate that no single certification can be relied upon to adequately test knowledge necessary to perform the responsibilities for each of the target job roles. As well, no mix of the analyzed certifications was deemed appropriate for a System Operator to understand key aspects of how cybersecurity impacts system operations. Of special note, the NERC SOC, which is focused on system reliability operations, does not currently cover any of the cybersecurity responsibilities identified for the four job roles. This highlights a growing concern as System Operators are surrounded by technology and rely on this technology as the tools to enable their work.

The results of mapping the workforce development resources (courses, certifications, and frameworks) to job responsibilities show that no combination of workforce programs is able to address the entire set of responsibilities to be fulfilled by the target job roles (see Figure 4.1). Using any one workforce program to guide personnel development planning, development, or certification will provide at best coverage of six of the job responsibility areas or 54% coverage. Applying two of the workforce programs might address seven of the job responsibility areas or 63%. Applying three programs will address eight of the job responsibility areas or 72%. Even if all four workforce programs are consulted, nine of the job responsibility areas, or 81%, will be touched upon, but as noted above, the two competency framework programs will provide greater emphasis on some areas not covered by the two workforce development programs, and vice versa. The results of the workforce development resources (courses, certifications, and frameworks) commonly provide emphasis for some job responsibilities, show

---

<sup>1</sup> Workforce credentialing programs refer to an authoritative body/organization providing a program to make sure that a certified individual has practical knowledge and skills in the identified areas of computer security or power system operations. Some organizations offer certification programs for job-specific responsibilities and others align to a body of knowledge. Knapp & Associates (Knapp & Associates 2007) states, “professional/personnel certification programs have become prevalent across diverse industries and occupations/professions, but there has been surprisingly little research conducted on these programs.” (The 2007 *Knapp Certification Industry Scan* is the most comprehensive study of the certification industry to date).

weaker emphasis in others, and possess unique responsibility emphasis, requiring an organization to embrace multiple resources, which will be further discussed in subsequent sections of this report.



**Figure 4.1.** Greatest Coverage of Job Responsibility Areas through Implementing Combinations of Workforce Frameworks



## 5.0 Implications

### 5.1 Implications for Electric Power Sector Entities

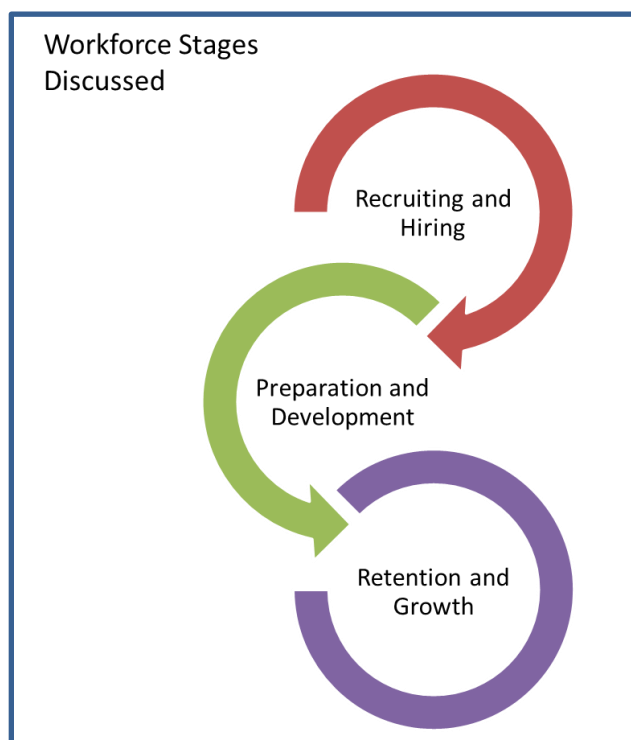
Members of the panel provided a number of valuable insights to what the data discovered in this phase of the effort meant to them and their respective organizations. Data obtained through the various panel activities was discussed by the panel members and validated based on the reality of the entity work environment. The panel discussions also further examined the data to determine whether there were near-term actionable data within the responses or entity practices that provided guidance for other entities to immediately implement in their efforts to manage through the workforce development issues. A variety of positions and comments were received based on the diverse positions that panel members represent: entity size, functions performed, sourcing strategy in use, organization structures, and entity awareness of current capability and maturity.

This lack of a standardized capability progression in cybersecurity for the electric power sector is highlighted by just such a progression that has developed with the advance of the NERC Certified System Operator. Twenty years ago Control Center operators were typically evaluated for a position based on the possession of a higher education degree or equivalent work experience. Once selected for an operator position, the individual was evaluated for preparedness and effectiveness through on-the-job training and performance management tools. Over time this was viewed as deficient and a program was developed to create formal training and credentialing. Utilities then moved to requiring System Operators to be NERC certified in order to fill specified positions with real-time reliability responsibilities. Over time enhancements have been added and now the same positions are required to obtain continuing education units and emergency operations training hours in order to retain the credential. Through this process there has been a natural maturity of the overall program along with numerous refinements to the preparation of potential candidates, the quality of ongoing training delivered and the testing criteria. Recent activity has further pursued a means to qualify an operator to perform a job, which now has reached sufficient maturity in the process to use the certification as the new baseline or cost of entry for specified roles and adds a series of qualification- and performance-based components to the process. The new NERC training standard PER-005 (NERC 2009) mandated that a *widely recognized* systematic approach to training be used to establish a formal training program for System Operators. Requirements in PER-005 called for job task analyses to be performed to identify each real-time reliability related task for each System Operator position. From these task lists training content and capability assessments are developed and implemented. This progression in operator workforce development is a model for the development path of the cybersecurity professional. Currently, as demonstrated by the Phase 2 effort of this study, the industry is at a stage where it is questioning whether the cyber certifications are teaching and testing the appropriate material, and is also identifying that the credentials should truly be a baseline or a cost of entry to be considered for a role rather than the end goal in a training program. Secondary qualification and training criteria need to be pursued to provide the same training progression and program maturity for the cybersecurity professional as currently exists for the System Operator role.

The panel explained the value of common certifications as indicators that individuals had invested energy and time in the general domains of cybersecurity. Some of those certifications were likened to a bachelor's degree as it indicated an achievement, but was not seen as a predictor of work performance or a fit for a specific function in a cybersecurity role. Much discussion occurred amongst panel members in regard to the capability indication of a certification. Further discussion focused on the need for a

cybersecurity skill assessment instrument that can be used as a second-level assessment beyond the certifications. The panel discussed further opportunities that exist for industry to partner with academic, government and research organizations to design an assessment instrument that the industry can use to guide recruitment, selection, development, and retention/performance evaluation.

Along with the general implications to the electric power sector addressed above, the panel identified implications to the current power utility efforts focused on recruiting, developing, and retaining a capable cybersecurity workforce. These implications are addressed in the following sections, which are organized by the stages in a workforce cycle (Figure 5.1).



**Figure 5.1.** Workforce Stages

### **Workforce Recruitment and Hiring**

Panel discussions indicated a common frustration in specifying valued competencies at a task execution level and difficulty in using comparable measures to determine the level of confidence that a particular candidate possesses the sought-after competencies. Entities are utilizing the course and credentialing tools they have available to evaluate and develop employees; however, even though candidates may have attended similar training and obtained the same certification credentials, employees may perform dramatically differently in a given role. The existing tools available in the credentialing space provide a measure of knowledge and may measure skill and ability depending on the credential; however, they do not measure the appropriate fit of an individual for a role. Some members of the panel have identified a need to further research the effectiveness of tools that try to identify the appropriate “fit”

of a candidate for a given role; for example, tools like the Five Factor Model<sup>1</sup> (or Big ‘5’ factors) which some organizations facing these specific “fit” challenges have implemented. The panel did not study this approach for the cybersecurity workforce needs, but believes this may be an area to conduct further research.

## Workforce Development and Preparation

Panel discussions focused on how organizations can plan and execute development programs to best equip their workforce with the knowledge, skills, and abilities that will translate into improved work performance and accomplish goals assigned to specific cybersecurity job roles. As addressed in the findings, (Section 3) none of the four workforce programs analyzed in this project completely addressed all of the job responsibilities necessary for power system cybersecurity. Even if an entity is utilizing all four of the workforce programs as resources to develop, maintain and guide the security workforce there would still be significant gaps in the workforce development areas. These results suggest that for utilities seeking to develop and maintain a prepared and well-trained security team<sup>2</sup> it would be important to understand the benefit these workforce programs can provide and be prepared to address the gaps. Currently, utilities must address the gaps in available workforce development programs through the creation and implementation of their own programs; however, the few attempts are plagued by lack of expertise, poor funding, and reliance on a key individual.

Entities can immediately take the roles identified to have strong alignment with available certifications of value and adjust job postings or training programs for staff in those roles. For the areas where strong alignment with an existing certification does not exist, entities can first adjust job descriptions and career paths to remove credential requirements that do not align with job-identified roles. Second, organizations can begin developing or working with partners to utilize training programs that do

Operations Technology has been a sticking point in my mind during this entire process, not just here specifically, but elsewhere (DOE, IEEE, etc.), as well. While the industry experiences this transitory phase of developing a “Smart Grid”, the “Smart” portion of security is receiving the bulk of the attention, and there seems to be less emphasis on the power end. For example, while the control systems (communications, device logic, firmware, controller software and definition files) for a generator control unit are highly computerized, “we” seem to be focused primarily on the areas that have been “historically” viewed as “information security”. This is partly out of necessity as these systems are now computer-controlled, while others are increasingly becoming more so. This does seem to be leaving an aspect of power generation control “in the dark” (no pun) during this process. Not every Linux server expert who understands server and network security will be willing (or, perhaps capable, to be honest) to understand the nuances of power generation, which requires other areas of expertise which border on the domain of physics (the relationship of changing electrical and magnetic fields, the concept of inertia in the bulk power system, capacitance, inductance, etc.) No newly minted BSEE (Bachelor of Science in Electrical Engineering) *really* understands those concepts, either.

- Joseph J. Januszewski, III, Panel Member

---

<sup>1</sup> Numerous psychological researchers have been associated with the Five Factor Model of Personality (also referred to as the Big 5 Factors) that described five broad trait dimensions including agreeableness, conscientiousness, emotional stability, extraversion and intellect. These five dimensions are contained in many pre-employment inventories used as applicant screening tools (Wiggins, 1996).

<sup>2</sup> “Security team” is an inclusive term used to describe the combination of designated security roles and technology or operation roles that address security. Smaller utilities either have a single security person or personnel with secondary duties in security that include being able to work with others to accomplish the security mission.

fill the identified gaps. Panel leadership believes these results confirm a common belief within entities that traditional IT roles are fairly well defined with credentials and available credentials, while OT roles do not have a well-defined alignment to existing programs.

The identified frameworks, which include strategic, long-term impact and tactical, short-term impact, are all in varied levels of use by workforce managers across the electric power sector. The degree to which they have been adopted and implemented varies greatly from entity to entity. The benefits entities will reap from the frameworks depend greatly on their current maturity level and the support received to pursue higher levels of maturity and capability. Leadership would traditionally look for assessment and framework approaches to gain a picture of the current environment performance, which would be a reflection of a number of components (investment, leadership buy-in, staffing allocations, staffing capabilities, current system capabilities and resilience). Based on this picture of the environment, leadership would then build initiatives to address the greatest gaps and then repeat the assessment at a determined frequency to make sure they are making strategic improvements. The course and certification frameworks are truly starting from the perspective of workforce development and improving the knowledge, skills, and abilities of the workforce that is in place, then utilizing certification and credentialing frameworks to validate the capabilities of an individual. This is a focus on the short-term needs of tactical staffing management, skill management, and current capability measures.

As an industry, electric power entities should consider whether the application of cybersecurity roles and the need to augment operations and engineering staff with specific cyber-related knowledge, skills, and abilities is unique enough to warrant sector-specific development resources. A certification tailored to energy OT systems would be a smart community investment. The difficulty comes in the management of courseware and certifications over time. NERC became the focal point for the development of a SOC and it was deemed a necessary tool to help provide a reliable power system and warranted the ongoing investment in maintaining the certification program. The results of this study further present a potential need to update the existing SOC domains to include some elements of underlying OT and cybersecurity knowledge essential to operating a reliable power system.

### **Workforce Retention and Future Pipeline Building**

Topics on workforce retention and attracting new entrants were not directly surveyed or pursued in the process of the Phase 2 effort; however there were discussions among entities around these topics. Specifically, the discussion focused on certain markets experiencing loss of skilled individuals to other sectors and decreasing levels of interest or awareness in regard to the cybersecurity needs of this sector from potential new entrants. Entities participating in the Phase 2 effort discussed a variety of initiatives, practices or thoughts. A summary list of topics discussed is captured below:

“While every company may say they want the top performer in every competency area, the math tells us that isn’t going to happen. And if they do get them, the top performers won’t likely stay very long as better offers come their way. For many utilities, it may be a goal to get some of these top performers for a few years on their way up to inspire the average and above average performers who are likely to stay longer.”

- Gilbert Sorebo, Panel Member

- The investment in a sector-specific workforce resource approach to include certification may result in a valued specialization that incentivizes individuals to remain within power system related jobs.

- Develop internship programs targeting placement of students into two-year and four-year cybersecurity curricula and scholarship programs that require a set term of service in the energy sector.
- Develop a mentoring structure based on expertise and technical competence levels for critical and highly differentiating work tasks, a program that extends outside of the organization.
- Make sure employer compensation departments are considering specialty skills of individuals in these roles when market comparisons are determined.

## Human Element in Determining Cyber Risk

“It is nevertheless axiomatic that nothing in business or government happens without a human doing it, ultimately. Human capital suffers from a variety of flaws and weaknesses; of a physical or mental/emotional kind. These facts expose the risk that what is the weakest link often finds itself in the position of “key man”, and becomes a potentially catastrophic Single Point of Failure (SPoF).”

- Ross Leo, Panel Member

We will now address one final thought about both the general cyber risk awareness of an organization’s staff, and more specifically, the competency inventory of the cybersecurity professionals and system operators. The traditional risk assessment program begins with taking an inventory of assets and processes, understanding the organization’s or business’s reliance on those assets and processes, and determining the hazards that can impact the productivity or functioning of those assets and processes. This is offset by evaluating the mitigations or controls that prevent or diminish the hazards from occurring and affecting the

organization. The Department of Energy, working with the electric power industry, developed the Cybersecurity Risk Management Process, an excellent resource to enhance risk management programs tailored to energy infrastructure (DOE 2013b).

A significant element of that process includes inventorying vulnerabilities that may allow a particular hazard to actualize or have a negative impact. We are familiar with inventorying technical weaknesses or physical gaps, and for physical security threats we try to calculate the capability and timeliness of the security response to evaluate the necessary security delay-detect-respond cycle. Many of the panel members recognize shortfalls in specific competencies as having an impact on their risk exposure. There are some emerging efforts to calculate the vulnerability that exists when comparing the competency

inventory/assessment of an entity’s cyber defense staff to cyber threats and particular tactics, techniques, and procedures. Entities should consider the competence of the cyber defense team (our research found that this group expands far past the Information Security Team and includes infrastructure and information technology support and system owners) as an element of their overall risk calculus.

With regard for what the organization can do to safeguard itself against adverse impacts due to losses in human capital (regardless of cause), there are some things that are effective in reducing impacts from such losses:

1. Identify critical skills, knowledge, experience in individuals and take steps to cross-train and replicate this in others (2 or 3 times)
2. Enforce a program of skills maintenance, even subsidize this program
3. Records must be kept on all critical data and made available to all concerned persons (with controlled distribution and Need to Know)
4. To some (rather fluid) extent, programs that build mutual loyalty between employers and workforce or in some way bind them together in a positive fashion may be an option

- Ross Leo, Panel Member

## 5.2 Implications for Competency Frameworks and Workforce Development

As discussed above, the results of the studies show that no combination of workforce programs is able to address the entire set of responsibilities to be fulfilled by the target job roles, and the two competency framework programs (NICE and ES-C2M2) will provide greater emphasis on some areas not covered by the two workforce development programs (certifications and courses), and vice versa. This makes it essential for an organization with limited ability to invest and implement all four workforce programs to instead make sure that they are selecting the combination of programs that address the job responsibility areas that provide guidance where the organization's needs are greatest. Thus, it is more important for an organization to first evaluate staff against the full JPM developed in Phase I. This will enable them to determine the profile of strengths and weaknesses by individual and team. Then, the organization may adopt the workforce programs that emphasize responsibility areas that will align with the mission and address the competency gaps of their workforce.

The significant gaps and misalignments among the workforce programs have several implications for developers of competency frameworks. First, our results replicated the findings from studies in related fields, such as systems engineering (Kasser et al. 2012), that demonstrate that a comprehensive competency model, grounded in job performance, brings clarity and direction to designing, assessing, or aligning workforce programs to industry, organization, or even an individual's unique requirements. Second, these results further suggest that competency frameworks, whether for role definition or maturity assessment, should be developed using established best practices in competency modeling. Campion et al. (2011) identified fifteen practices that guided the methodology used in the two phases of this project. The results show support for these best practices, and suggest that their adoption by existing cybersecurity competency framework developers could enhance a strong, beginning foundation for guiding power systems cybersecurity workforce development. Current cybersecurity competency frameworks have stressed breadth over depth. Consequently, they provide excellent descriptions of the categories of jobs or areas in which assessment may be helpful in determining the level of maturity. However, to better align and provide more specific direction to workforce development, these efforts should limit further expansion of breadth and emphasize greater depth in elaborating these models to include the context (vignettes or use cases), mission (goals and objectives), requirements (responsibilities) and, most importantly, the critical and differentiating job tasks that will assist in validating both the scope of responsibilities and the indicators for proficiency (knowledge), performance (skill), or aptitude (ability) assessments and certifications.

Similarly, the results of this study have several implications for developers of workforce development programs. First, education, training and certification programs should document how their curriculum's learning objectives align with the job responsibilities emphasized in the competency frameworks. This would include stating explicitly the job role(s) and/or the specific responsibilities of that job which the program is targeted to improve or assess. Second, development programs should align their outcomes with these same responsibilities. For instance, exam items would be developed and validated to measure knowledge, skill, and ability to perform the tasks included in a responsibility area. Further, rather than providing the student with a summative score—a grade or a pass/fail based on an overall cutoff score—a student should receive a profile report indicating areas of strength and weakness in executing the tasks necessary to fulfill the target responsibility. This competency profile would enable both individuals and their organizations to better map and align future development with those programs designed to address

gaps shown through these formative assessments. Third, program descriptions and outcome results should specify the level of expertise (Benner 2004; Dreyfus and Dreyfus 1980). Programs designed for beginners should demonstrate that they are covering the fundamental responsibilities and tasks. Likewise, programs designed for development of competent or expert practitioners should demonstrate that they are emphasizing those differentiating responsibilities and tasks. Finally, program effectiveness evaluation should be based on a demonstration of either breadth or depth of competency profile improvement according to how the program is aligned with the job performance model for the targeted job role.

### **5.3 Implications for Further Research**

The results of the job role responsibility mapping indicate that substantial additional research is required to address gaps and align the focus of these important cybersecurity competency programs. Perhaps much of the misalignment may have resulted from the lack of a detailed job performance model (such as that produced in Phase I of this project). The gap and overlap mapping identified here were not possible prior to the availability of a detailed list of job responsibilities, validated by being grounded in current lessons learned from the field, specifying the job role tasks and performance levels (objective) required to address critical and differentiating use cases. Further, identifying the fundamental and differentiating tasks in a job performance model may help to determine the position of an individual or team along the expertise development curve. Consequently, future research should both seek to validate the predictive accuracy of the job performance model and apply a validated model to accredit workforce programs based on the job role(s), responsibility areas and expertise level at which they are targeted. Additionally, future research would seek to develop individual and/or organizational self-assessments that help answer questions related to designing a holistic approach to workforce development such as that outlined in the Ground Truth Expertise Development model (Assante and Tobey 2011) that provides the theoretical framework for the present study:

- To what degree does an individual or team feel they can perform the responsibilities of the NICE functional roles?
- How mature are staff capabilities to meet the objectives identified by the ES-C2M2?
- What certifications are likely to best inform independent analysis of proficiency based on job role or organization-specific responsibility assignments?
- What education and training programs should be given priority in an individual or team-based development plan?

#### **What Would a Comprehensive Workforce Framework Look Like?**

More research is needed to develop a comprehensive framework for cybersecurity workforce planning and talent management. Cybersecurity is a discipline in which judgment and decisions must be made under tremendous stress and time constraints in novel or rare conditions and where the context is constantly shifting, information is often lacking or conflicting, and there is often no single best procedure or clearly optimal outcome. Such environments are called competency-based domains (Smith et al. 2004) because the difference between novices and experts is related to how quickly they gain situational awareness (Endsley and Garland 2000), and how well they reflect on their thought processes, (their metacognition), rather than simple cognitive recall of facts or their general intelligence. Accordingly, a comprehensive workforce framework should detail not only the roles; responsibilities; tasks; and

knowledge, skills, and abilities; but should identify the decision processes and methodological procedures and tools that determine effective performance.

In other complex competency-based domains, such as aviation, medicine or weather forecasting, the competency models and workforce development programs are built upon detailed human-factor studies. A comprehensive framework can therefore be used to establish performance-based standards for education, proficiency and skill certification, as well as evidence-based quality standards of care for an entire profession. An additional advantage of these comprehensive frameworks is that they not only model best practice, but they can also explain and predict errors. This is most notable in the development of comprehensive workforce frameworks for pilots (Wiegmann et al. 2001). A defining characteristic of these workforce frameworks is that role definition, maturity assessment, training, and certification are all based on a common performance model. As discussed above, the existence of a robust job performance model has been proposed as the primary indicator of the highest level of competency framework maturity (Kasser et al. 2012).



## 6.0 Conclusion

Implementation of the smart grid provides mechanisms for managing consumers' use of power as well as its generation, transmission and distribution. However, the underlying cyber infrastructure, essential to the operation of the smart grid, must be secure. As an industry, the development of a standard framework for educating and certifying those personnel entrusted with these responsibilities is essential. This need is highlighted by the gaps in development programs and resources and must be addressed in the near term to successfully integrate a truly secure smart grid.

This report ties together three studies that asked both an SME panel and community practitioners to analyze the value, commonality, and mapping of certification exams, cybersecurity frameworks, and workforce development programs to power system cybersecurity job role responsibilities. These studies collectively showed that the JPM provides sufficient detail to derive insights about the gaps, overlaps and maturity of workforce programs. The analysis of certifications yielded nine vendor-neutral certifications that most panel members indicated were valuable for determining job competence. The results of the certification review indicate that no single certification can be relied upon to adequately test knowledge necessary to perform the responsibilities for each of the target job roles. The panel considered the System Operator role, as it represents a functional power system-focused role that has received tailored attention through the industry-developed NERC SOC. The panel found that despite being considered a valuable certification, the NERC SOC does not currently cover any of the cybersecurity responsibilities identified with the four job roles. The panel felt that operational and engineering job roles need to consider the applicable cybersecurity knowledge necessary for the performance of their functions and to integrate with cybersecurity-specific roles to enhance the security and incident response capability of the power system.

The mapping demonstrated that the frameworks that were analyzed had areas of misalignment that may have resulted because these workforce programs did not share a common, underlying model of job performance as was developed in the first phase of this project. These findings can be translated into action by power system entities. First, entities can immediately use the roles identified to have strong alignment with available certifications of value to adjust job postings or training programs for staff in those roles. Second, for the areas where strong alignment with an existing certification does not exist, entities can first adjust job descriptions and career paths to remove credential requirements that do not align with job-identified roles. Third, organizations can begin developing or working with partners to utilize training programs that best fill the identified gaps.

Panel leadership believes these results confirm a common belief within entities that traditional IT roles are fairly well defined with credentials and available credentials, while OT roles do not have a well-defined alignment to existing programs. Panel discussions indicated a common frustration among the panel members in specifying valued competencies at a task execution level and difficulty in using comparable measures to determine the level of confidence that a particular candidate possesses the sought-after competencies. This is evident in the electric power sector, as many power system entities have seen the progression of the NERC Certified System Operator advance over the years. A similar capability progression is needed in the power cybersecurity space.

As an industry, electric power system entities should consider whether the application of cybersecurity roles and the need to augment operations and engineering staff with specific cyber-related knowledge, skills, and abilities is unique enough to warrant sector-specific development resources. A

certification tailored to cybersecurity of energy OT systems is a smart community investment. On a final note, a compelling argument is made that power system entities should evaluate the competence of their extended cyber defense team as an element of their overall risk calculus. The continued implementation of digital technology into every aspect of power systems helps us reach the goal of a fully integrated power system without boundaries—from end to end, generation to distribution. It is incumbent on power system entities and key stakeholders to actively redefine critical power system job functions to field a workforce that can tackle the cybersecurity challenges of this new edgeless power system.

## 7.0 References

- Assante MJ and DH Tobey. 2011. "Enhancing the cybersecurity workforce." *IEEE IT Professional* 13, 12–15.
- Benner PE. 2004. "Using the Dreyfus model of skill acquisition to describe and interpret skill acquisition and clinical judgment in nursing practice and education." *Bulletin of Science, Technology and Society* 24, 188–199.
- Bishop M and S Engle. 2006. "The software assurance CBK and university curricula." In *Proceedings of the 10th Colloquium for Information Systems Security Education* (pp. 14–21). Adelphi, MD. Retrieved from <http://nob.cs.ucdavis.edu/~bishop/papers/2006-cisse-1/swacbk.pdf>.
- Boje DM. 2001. *Narrative Methods for Organizational and Communication Research*. London: Sage Publications.
- Boudreau JW and PM Ramstad. 2005. Talentship, talent segmentation, and sustainability: A new HR decision science paradigm for a new strategy definition. In: MR Losey, SR Meisinger, and D Ulrich (Eds.), *The future of human resource management: 64 thought leaders explore the critical HR issues of today and tomorrow* (pp. 293–304). Hoboken, N.J.: Society for Human Resource Management.
- Campion MA, AA Fink, BJ Ruggenberg, L Carr, GM Phillips, and RB Odman. 2011. "Doing competencies well: Best practices in competency modeling." *Personnel Psychology* 64, 225–262.
- CSIS – Center for Strategic and International Studies. 2010. "A human capital crisis in cybersecurity: Technical proficiency matters." p. 53. CSIS Commission on Cybersecurity for the 44th Presidency. Washington, D.C.
- DOE – U.S. Department of Energy. 2013a. *Energy Systems Cybersecurity Capability Maturity Model*. Accessed July 31, 2013, at <http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model> (undated webpage).
- DOE – U.S. Department of Energy. 2013b. Cybersecurity Risk Management Process (RMP). Accessed July 30, 2013 at <http://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp> (undated webpage).
- Dreyfus SE and HL Dreyfus. 1980. *A five-stage model of the mental activities involved in directed skill acquisition*. Air Force Office of Scientific Research, Berkeley, CA.
- Endsley MR and DJ Garland. 2000. *Situation awareness: Analysis and measurement*. Lawrence Erlbaum Associates, Mahwah, NJ.
- Flanagan JC. 1954. "The critical incident technique." *Psychological Bulletin* 51 327–358.
- Fleiss JL. 1971. "Measuring nominal scale agreement among many raters." *Psychological Bulletin* 76(5), 378–382. doi:10.1037/h0031619.

- Fleiss JL and J Cuzick. 1979. "The reliability of dichotomous judgments: Unequal numbers of judges per subject." *Applied Psychological Measurement* 3(4), 537–542.
- Holley JW and JP Guilford. 1964. "A note on the G index of agreement." *Educational and Psychological Measurement* 24, 749–753.
- Holley JW and GA Lienert. 1974. "The G index of agreement in multiple ratings." *Educational and Psychological Measurement* 34(4), 817–822. doi:10.1177/001316447403400409.
- Kasser J, D Hitchins, M Frank, and YY Zhao. 2012. "A framework for benchmarking competency assessment models." *Systems Engineering* 16(5), 29–44.
- Klein GA, R Calderwood, and D MacGregor. 1989. "Critical decision method for eliciting knowledge." *IEEE Transactions on Systems, Man and Cybernetics* 19(3), 462–472.
- Knapp & Associates. 2007. *Knapp Certification Industry Scan*. Knapp & Associates International, Inc., Princeton, New Jersey. Accessed July 30, 2013 at <http://www.knappinternational.com/assets/uploads/pages/Knapp%202007%20Industry%20Scan%20Report.pdf>.
- Landis JR and GG Koch. 1977. "The measurement of observer agreement for categorical data." *Biometrics* 33, 159–174.
- Moore, S., and DW White. 2012. *Electricity Subsector Cybersecurity Capability Maturity Model, Version 1.0* (p. 84). U.S. Department of Energy. Retrieved from <http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf>
- NICE – National Initiative for Cybersecurity Education. 2012. *National Cybersecurity Workforce Framework*. Accessed July 31, 2013 at [http://csrc.nist.gov/nice/framework/national\\_cybersecurity\\_workforce\\_framework\\_v1\\_1\\_august2012\\_for\\_printing.pdf](http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_v1_1_august2012_for_printing.pdf).
- NIST – National Institute of Standards and Technology. 2011. NICE Cybersecurity Workforce Framework. Retrieved from <http://csrc.nist.gov/nice/framework/>
- NERC – North American Electric Reliability Corporation. 2009. *System Personnel Training*. Atlanta, GA. Accessed July 30, 2013 at <http://www.nerc.com/files/PER-005-1.pdf>.
- NERC – North American Electric Reliability Corporation. 2010. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. Atlanta, GA. Accessed July 31, 2013 at <http://www.nerc.com/files/HILF.pdf>.
- NERC – North American Electric Reliability Corporation. 2012a. *2012 Long-Term Reliability Assessment* (p. 335). Atlanta, GA. Accessed July 31, 2013 at [http://www.nerc.com/files/2012\\_LTRA\\_FINAL.pdf](http://www.nerc.com/files/2012_LTRA_FINAL.pdf).

NERC – North American Electric Reliability Corporation. 2012b. *Cyber Attack Task Force: Final report* (p. 76). Atlanta, GA. Accessed July 31, 2013 at [http://www.nerc.com/docs/cip/catf/12-CATF\\_Final\\_Report\\_BOT\\_clean\\_Mar\\_26\\_2012-Board%20Accepted%200521.pdf](http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf).

NERC – North American Electric Reliability Corporation. *System Operator Certification*. Accessed April 27, 2013, at <http://www.nerc.com/page.php?cid=6%7C84> (undated webpage).

O’Neil LR, MJ Assante, and DH Tobey. 2012. “Smart Grid Cybersecurity: Job Performance Model Report” PNNL-21639 Pacific Northwest National Laboratory, Richland, Washington. Accessed July 31, 2013 at <http://energy.gov/oe/downloads/smart-grid-cybersecurity-job-performance-model-report-and-phase-1-overview-august-2012>.

Paulsen C, E McDuffie, W Newhouse and P Toth. 2012. NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy*, May 2012, p.76–79.

Pliske RM, B Crandall, and G Klein. 2004. “Competence in weather forecasting.” In K Smith, J Shanteau, and P Johnson (Eds.), *Psychological investigations of competence in decision making*. (pp. 40–68) Cambridge University Press, Cambridge, UK.

Schweitzer D, J Humphries, and L Baird. 2006. “Meeting the criteria for a Center of Academic Excellence (CAE) in information assurance education.” *Journal of Computing Sciences in Colleges* 22(1), 151–160.

Smith K, J Shanteau, and P Johnson. 2004. “Introduction: What does it mean to be competent?” In K Smith, J Shanteau, and P Johnson (Eds.), *Psychological investigations of competence in decision making*, (pp. 1–4). Cambridge University Press, Cambridge, UK.

Theoharidou M and D Gritzalis. 2007. “Common body of knowledge for information security.” *IEEE Security and Privacy* 5(2), 64–67.

Tobey DH. 2007. “Narrative’s Arrow: Story sequences and organizational trajectories in founding stories.” In *Standing Conference on Management and Organizational Inquiry*. Las Vegas, NV.

Towhidnejad M, TLJ Ferris, A Squires, and R Madachy. 2013. “Enabling systems engineering program outcomes via systems engineering body of knowledge.” *Procedia Computer Science* 16, 983–989.

Wiegmann DA, SA Shappell, and United States. Office of Aviation Medicine. 2001. *A human error analysis of commercial aviation accidents using the human factors analysis and classification system (HFACS): Final report*. U.S. Dept. of Transportation, Federal Aviation Administration, Office of Aviation Medicine; Washington, D.C.; Springfield, VA. Available to the public through the National Technical Information Service.

Wiggins J. 1996. *The Five-Factor Model of Personality*. Guilford Publications, New York.

Wu, Y., H Siy and R Gandhi. 2011. Empirical results on the study of software vulnerabilities. In *Proceedings of the International Conference on Software Engineering* (pp. 964–967). Presented at the ICSE 2011, Honolulu, HI: Association for Computing Machinery.



## **Appendix A**

### **Smart Grid Cybersecurity (SGC) Panel Roster**





## Appendix A

### Smart Grid Cybersecurity (SGC) Panel Roster

(As of 29 April 2013)

#### OFFICERS

Conway, Tim (Chair)	NiSource/SANS	Industry
Perman, Karl (Vice-Chair)	North American Transmission Forum	Industry

#### NBISE CONTRIBUTOR

Assante, Michael	National Board of Information Security Examiners	Research
------------------	--	----------

#### PANEL MEMBERS

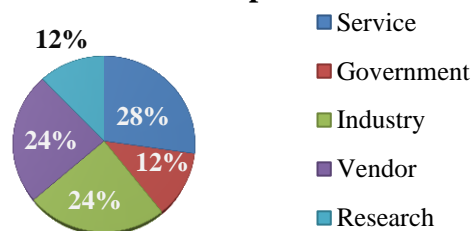
Aber, Lee	OPower	Industry
Agrawal, Sandeep	Neilsoft Limited	Service
Akyol, Bora	Pacific Northwest National Laboratory	Research
Arumugam, Balusamy	Infosys	Vendor
Chamberlin, Leonard	FERC (Office of Electric Reliability)	Government
Christopher, Jason	Federal Energy Regulatory Commission	Government
Damm, Benjamin	Silver Springs Network	Vendor
Fansler, Aaron	Northrup Grumman	Vendor
Hayden, Maria	Pentagon	Government
Januszewski, Joseph	Consultant	Service
Keller, Steven	Southwest Power Pool Regional Entity	Industry
Kersey, Karl	Schneider Electric	Vendor
Leo, Ross	Consultant	Vendor
Luallen, Matthew	Industry Contractor	Service
Miller, Patrick	Energy Sec	Industry
Morris, Donald	CenterPoint Energy	Industry
Perez, Gilbert	The Structure Group	Vendor
Rasche, Galen A.	Electric Power Research Institute	Research
Sample, James	Pacific Gas and Electric Company	Industry
Sawall, Chris	Ameren	Industry
Scott, Anthony David	Accenture	Service
Skare, Paul	PNNL	Government
Sorebo, Gilbert	Science Applications International Corporation	Service
Strickland, Thomas	KEMA	Service
Terebussy, Michael	CISCO	Service
Thanos, Dan	GE Digital Energy	Vendor
Tydings, Kevin	SAIC	Service
Weber, Donald	InGuardians	Vendor
Wenstrom, Mike	Mike Wenstrom Development Partners	Service
Yardley, Tim	University of Illinois	Research

#### Contributor Statistics

<b>Contributors:</b>	<b>33</b>
Industry:	8
Service:	9
Government:	4
Vendor:	8
Research:	4

\* Two members (not listed above) asked to be removed from the panel in 2012; neither had participated in any activities of Phase 2.

#### Sector Participation





## **Appendix B**

### **Panel Meetings and Activities for Phase 2**



## Appendix B

### Panel Meetings and Activities for Phase 2

#### **PANEL MEETINGS/SESSIONS**

#### **DATE**

Smart Grid Cybersecurity (SGC) Panel	
Kick-off Meeting, Option 1	12 September 2012
SGC Panel Kick-off Meeting, Option 2	13 September 2012
Work Session 1	31 October 2012
Work Session 2, Option 1	7 November 2012
Work Session 2, Option 2	8 November 2012
Work Session 3	16 November 2012
Work Session 4	28 November 2012
Work Session 5	19 December 2012
Final Panel Discussion	16 April 2013

#### **PANEL ACTIVITY**

#### **PARTICIPATION**

#### **RATE**

Rate importance of certifications	6	18.2%
Elicit target job roles	17	51.5%
Assign responsibilities to job role	17	51.5%
Assign certifications to job roles	16	48.5%
Assign certification domains to responsibility areas	5	15.2%
Assign National Initiative for Cybersecurity	22	66.7%
Education tasks to responsibility areas		
Assign Electric Subsector Cybersecurity Capability	20	60.6%
Maturity Model objectives to responsibility areas		
Assign course topics to responsibility areas	23	69.7%
<i>Mean Number of Participants</i>	<i>15.75</i>	<i>47.7%</i>



## **Appendix C**

### **Certifications and Rating Results**





## Appendix C

### Certifications and Rating Results

This appendix provides the results of the subject matter expert (SME) panel's first activity to rate the importance of certifications for assessing competence in the target job roles. The table shows the 64 certifications presented to each panel respondent. For each certification, the respondent indicated whether they thought the certification was common or uncommon for incumbents in power system cybersecurity job roles, and whether such certification was valuable for assessing competence. The certifications in the list below are ordered by the "Valuable" rating they received from the subject matter expert panel. The name included in the parentheses is the certification organization.

Certifications	Common	Uncommon	Valuable
CISSP – Certified Information Systems Security Professional (ISC) <sup>2</sup>	16	1	14
CCNP Security – Cisco Certified Network Professional (Cisco)	12	6	12
SOC – System Operator Certification (NERC)	10	6	12
CCIE Security – Cisco Certified Internetwork Expert (Cisco)	7	10	11
CEH – Certified Ethical Hacker (EC-Council)	5	11	11
GPEN – Penetration Tester (GIAC)	1	13	11
CCNA Security – Cisco Certified Network Associate (Cisco)	14	3	10
CCSP – Cisco Certified Security Professional (Cisco)	11	5	10
CISA – Certified Information Security Auditor (ISACA)	12	6	10
CISM – Certified Information Security Manager (ISACA)	11	6	10
CRISC – Certified in Risk and Information Systems Control (ISACA)	4	13	10
GCIA – Certified Intrusion Analyst (GIAC)	3	14	10
GCIH – Certified Incident Handler (GIAC)	3	14	10
GWAPT – Web Application Penetration Tester (GIAC)	0	15	10
GCUX – Certified UNIX Security Administrator (GIAC)	4	14	9
GSNA – Systems and Network Auditor (GIAC)	0	16	9
GWAPT – Web Application Penetration Tester (GIAC)	0	16	9
GXPEN – Exploit Researcher and Advanced Penetration Tester (GIAC)	1	15	9
CWSP – Certified Wireless Security Professional (CWNP)	2	14	8
GAWN – Assessing and Auditing Wireless Networking (GIAC)	1	15	8
GCFE – Certified Forensic Examiner (GIAC)	1	16	8
GCFW – Certified Firewall Analyst (GIAC)	2	14	8
GCFA – Certified Forensic Analyst (GIAC)	3	14	8
GISF – Information Security Fundamentals (GIAC)	3	14	8
ISSEP – Information Systems Security Engineering Professional (ISC) <sup>2</sup>	2	15	8
ITIL – Information Technology Infrastructure Library (ITIL)	6	9	8
Security+ – CompTIA Security+ (CompTIA)	9	8	8
CHFI – Certified Hacking Forensic Investigator (EC-Council)	0	17	7
CSDP – Certified Software Development Professional (IEEE)	1	17	7
CWNA – Certified Wireless Network Administrator (CWNP)	4	13	7
GCED – Certified Enterprise Defender (GIAC)	0	17	7
GCWN – Certified Windows Security Administrator (GIAC)	3	14	7
GSEC – Security Essentials (GIAC)	5	11	7
ICND-2 – Interconnecting Networking Devices Part 2 (Cisco)	9	9	7
ISSAP – Information Systems Security Architecture Professional (ISC) <sup>2</sup>	3	14	7
ISSMP – Information Systems Security Management Professional (ISC) <sup>2</sup>	4	12	7
Network+ – CompTIA Network+ (CompTIA)	8	10	7
RHCSA – Red Hat Certified System Administrator (Red Hat)	8	9	7

<b>Certifications</b>	<b>Common</b>	<b>Uncommon</b>	<b>Valuable</b>
SCNP – Security Certified Network Professional (SCP)	4	14	7
GSLC – Security Leadership (GIAC)	1	17	6
GSSP-.NET – Secure Software Programmer-.NET (GIAC)	0	17	6
ICND-1 – Interconnecting Networking Devices Part 1 (Cisco)	8	9	6
ISA-CAP – ISA Certified Automation Professional (ISA)	4	13	6
OSCP – Offensive Security Certified Professional	0	16	6
SCNS – Security Certified Network Specialist (SCP)	4	13	6
CGEIT – Certified in the Governance of Enterprise IT (ISACA)	0	17	5
CSSLP – Certified Secure Software Lifecycle Professional (ISC) <sup>2</sup>	2	15	5
G2790 – Certified ISO-27000 Specialist (GIAC)	1	17	5
GISP – Information Security Professional (GIAC)	3	15	5
GSSP-JAVA – Secure Software Programmer-Java (GIAC)	1	17	5
CSDA – Certified Software Development Associate (IEEE)	1	17	4
GLEG – Legal Issues in Information Technology & Security (GIAC)	0	16	4
GWEB – Certified Web Application Defender (GIAC)	1	17	4
SSCP – Systems Security Certified Practitioner (ISC) <sup>2</sup>	3	15	4
CAP – Certified Authorization Professional (ISC) <sup>2</sup>	2	16	3
CCE – Certified Computer Examiner (ISFCE)	2	16	3
GREM – Reverse Engineering Malware (GIAC)	1	17	3
A+ – CompTIA A+ (CompTIA)	9	9	2
CNE – Certified Novell Engineer (Novell)	1	16	2
GCPM – Certified Project Manager (GIAC)	0	17	2
IC3 – Internet and Computing Core Certification (Certiport)	1	15	2
MCSA70-291 – Microsoft 70-291 (Microsoft)	7	10	2
CPT – Certified Performance Technologist (ISPI)	1	17	1
MCSA70-290 – Microsoft 70-290 (Microsoft)	8	9	1

## **Appendix D**

### **Module Public Participant Demographics**



## Appendix D

### Module Public Participant Demographics

This appendix includes the demographic information about the 41 individuals who participated in the public review and comment system (RaCS). These results were provided by each participant through their participation in the demographics survey prior to completing any of the RaCS modules. All data included is from individuals who completed at least one module in the RaCS.

Total modules completed: **108**  
 Number of module participants: **41**  
 Average # of modules completed per participant: **2.6**

Job Title	Number	Percent
Cyber Security Analyst	12	29.27%
Cyber Security Executive	8	19.51%
Cyber Security Manager	7	17.07%
Control Systems Manager	2	4.88%
IT Executive	2	4.88%
Control Systems Operator	1	2.44%
Cyber Security Operations Staff	1	2.44%
IT Professional	1	2.44%
Training Specialist	1	2.44%
Other	6	14.63%

Age	Number	Percent
21-30	3	7.69%
31-40	9	23.08%
41-50	14	35.90%
51-60	11	28.21%
Over 60	2	5.13%

Expertise in Cybersecurity Field	Number	Percent
Novice	0	0.00%
Beginner	1	2.44%
Proficient	16	39.02%
Competent	8	19.51%
Expert	16	39.02%

Familiarity with Smart Grid Cybersecurity	Number	Percent
Novice	7	17.07%
Beginner	8	19.51%
Proficient	13	31.71%
Competent	9	21.95%
Expert	4	9.76%

**Novice:** Minimal knowledge, no connection to practice

**Beginner:** Working knowledge of key aspects of practice

**Proficient:** Good working and background knowledge of the area

**Competent:** Depth of understanding of discipline and area of practice

**Expert:** Authoritative knowledge of discipline and deep tacit understanding across area of practice


Participant works for:	Number	Percent
Traditional Utility	28	68%
Integrator	3	7%
ISO/RTO or Market Operator	1	2%
Power System Supplier	1	2%
Other	8	20%


Certifications held	Number	Percent
CISSP	22	53.7%
CISA	8	19.5%
CISM	7	17.1%
CCNA	4	9.8%
CEH	3	7.3%
CRISC	3	7.3%
ISSAP	3	7.3%
Network+	3	7.3%
Security+	3	7.3%
A+	2	4.9%
CCSP	2	4.9%
GCIH	2	4.9%
GSEC	2	4.9%
GSLC	2	4.9%
ITIL	2	4.9%
CAP	1	2.4%
CCE	1	2.4%
CCIE	1	2.4%
CCNP	1	2.4%
CGEIT	1	2.4%
CHFI	1	2.4%
CNE	1	2.4%
GPEN	1	2.4%
ISSEP	1	2.4%
ISSMP	1	2.4%
MCSA70-290	1	2.4%
MCSA70-291	1	2.4%
SOC	1	2.4%

Gender	Number	Percent
Female	5	12%
Male	36	88%

## D.1 RaCS Demographic Survey

This section provides a screenshot of the demographic survey presented to all public participants prior to their participation in the RaCS.


**NBISE**  
NATIONAL BOARD OF INFORMATION  
SECURITY EXAMINERS



**Pacific Northwest**  
NATIONAL LABORATORY  
*Proudly Operated by **Battelle** Since 1965*

**Secure Power Systems Personnel Project  
Review & Comment System**

This Review & Comment System (RaCS) is an important step toward developing a deeper understanding of the resources available to enhance the cybersecurity workforce for power systems. The RaCS allows you to provide your feedback on the results of the Smart Grid Cybersecurity (SGC) panel's efforts to map job responsibility areas to four workforce development programs for power systems cybersecurity: certifications, training & education programs, the NICE framework, and the ES-C2M2 framework. *(Click on the Mapping Diagram on the right to enlarge.)*



\*Mapping exercises will help provide understanding of how certifications, NICE framework, ES-C2M2 framework, and training & education program topics align with the job responsibilities identified in SGC Phase 1.

**Prior to beginning your review, please complete this demographic survey.**

Responses are anonymous and will not be linked to your email address.

How many employees work at your facility?

Do you work for:

What job title best describes you?

How long have you held this position?

How many people report directly to you?

What job title best describes the position you had prior to your current job?

How would you classify your level of expertise in the cyber security field?

What level of familiarity do you have with smart grid operations?

What level of familiarity do you have with smart grid cyber security?

## RaCS Demographic Survey (Continued)

### Which, if any, certifications do you posses?

- ☐ A+ - CompTIA A+ (CompTIA)
- ☐ CAP - Certified Authorization Professional (ISC)<sup>2</sup>
- ☐ CCE - Certified Computer Examiner (ISFCE)
- ☐ CCIE Security - Cisco Certified Internetwork Expert (Cisco)
- ☐ CCNA Security - Cisco Certified Network Associate (Cisco)
- ☐ CCNP Security - Cisco Certified Network Professional (Cisco)
- ☐ CCSP - Cisco Certified Security Professional (Cisco)
- ☐ CEH - Certified Ethical Hacker (EC-Council)
- ☐ CGEIT - Certified in the Governance of Enterprise IT (ISACA)
- ☐ CHFI - Certified Hacking Forensic Investigator (EC-Council)
- ☐ CISA - Certified information Security Auditor (ISACA)
- ☐ CISM - Certified Information Security Manager (ISACA)
- ☐ CISSP - Certified Information Systems Security Professional (ISC)<sup>2</sup>
- ☐ CNE - Certified Novell Engineer (Novell)
- ☐ CPT - Certified Performance Technologist (ISPI)
- ☐ CRISC - Certified in Risk and Information Systems Control (ISACA)
- ☐ CSDA - Certified Software Development Associate (IEEE)
- ☐ CSDP - Certified Software Development Professional (IEEE)
- ☐ CSSLP - Certified Secure Softward Lifecycle Professional (ISC)<sup>2</sup>
- ☐ CWNA - Certified Wireless Network Administrator (CWNP)
- ☐ CWSP - Certified Wireless Security Professional (CWNP)
- ☐ G2790 - GIAC Certified ISO-27000 Specialist (GIAC)
- ☐ GAWN - GIAC Assessing and Auditing Wireless Networking (GIAC)
- ☐ GCED - GIAC Certified Enterprise Defender (GIAC)
- ☐ GCFE - GIAC Certified Forensic Examiner (GIAC)
- ☐ GCFW - GIAC Certified Firewall Analyst (GIAC)
- ☐ GCIA - GIAC Certified Intrusion Analyst (GIAC)
- ☐ GCIH - GIAC Certified Incident Handler (GIAC)
- ☐ GCPA - GIAC Certified Forensic Analyst (GIAC)
- ☐ GCPM - GIAC Certified Project Manager (GIAC)
- ☐ GCUX - GIAC Certified UNIX Security Administrator (GIAC)
- ☐ GCWN - GIAC Certified Windows Security Administrator (GIAC)
- ☐ GISF - GIAC Information Security Fundamentals (GIAC)
- ☐ GISP - GIAC Information Security Professional (GIAC)
- ☐ GLEG - GIAC Legal Issues in Information Technology & Security (GIAC)
- ☐ GPEN - GIAC Penetration Tester (GIAC)
- ☐ GPEN - GIAC Penetration Tester (GIAC)
- ☐ GREM - GIAC Reverse Engineering Malware (GIAC)
- ☐ GSEC - GIAC Security Essentials (GIAC)
- ☐ GSLC - GIAC Security Leadership (GIAC)
- ☐ GSNA - GIAC Systems and Network Auditor (GIAC)
- ☐ GSSP-.NET - GIAC Secure Software Programmer-.NET (GIAC)
- ☐ GSSP-JAVA - GIAC Secure Software Programmer-Java (GIAC)
- ☐ GWAPT - GIAC Web Application Penetration Tester (GIAC)

## RaCS Demographic Survey (Continued)

- ☐ GWEB - GIAC Certified Web Application Defender (GIAC)
- ☐ GXPEN - GIAC Exploit Researcher and Advanced Penetration Tester (GIAC)
- ☐ IC3 - Internet and Computing Core Certification (Certiport)
- ☐ ICND-1 - Interconnecting Networking Devices Part 1 (Cisco)
- ☐ ICND-2 - Interconnecting Networking Devices Part 2 (Cisco)
- ☐ ISA-CAP - ISA Certified Automation Professional (ISA)
- ☐ ISSAP - Information Systems Security Architecture Professional (ISC)<sup>2</sup>
- ☐ ISSEP - Information Systems Security Engineering Professional (ISC)<sup>2</sup>
- ☐ ISSMP - Information Systems Security Management Professional (ISC)<sup>2</sup>
- ☐ ITIL - Information Technology Infrastructure Library (ITIL)
- ☐ MCSA70-290 - Microsoft 70-290 (Microsoft)
- ☐ MCSA70-291 - Microsoft 70-291 (Microsoft)
- ☐ Network+ - CompTIA Network+ (CompTIA)
- ☐ OSCP - Offensive Security Certified Professional
- ☐ RHCSA - Red Hat Certified System Administrator (Red Hat)
- ☐ SCNP - Security Certified Network Professional (SCP)
- ☐ SCNS - Security Certified Network Specialist (SCP)
- ☐ Security+ - CompTIA Security+ (CompTIA)
- ☐ SOC - System Operator Certification (NERC)
- ☐ SSCP - Systems Security Certified Practitioner (ISC)<sup>2</sup>
- ☐ Other

What is your gender?

What is your age?

Continue

### Your privacy

This review and comment system is anonymous. The record kept of your module responses does not contain any identifying information about you unless a specific question in the module has asked for this. If you have responded to a module that used an identifying token to allow you to access the module, you can rest assured that the identifying token is not kept with your responses. It is managed in a separate database, and will only be updated to indicate that you have (or haven't) completed this module. There is no way of matching identification tokens with module responses in this review and comment system.

Powered with  by  © 2013



## **Appendix E**

### **Results and Analysis of Targeted Workforce Program Mapping to Job Responsibility Areas**



## Appendix E

### Results and Analysis of Targeted Workforce Program Mapping to Job Responsibility Areas

Based on the combined results of the Smart Grid Cybersecurity (SGC) panel and public review and comment system (RaCS) participants, the following workforce frameworks were determined to emphasize the following job responsibility areas:

- The National Initiative for Cybersecurity Education (NICE) framework emphasizes 5 of the 11 job responsibility areas:
  - Analyze security incidents.
  - Assess and manage risk.
  - Communicate results.
  - Identify and mitigate vulnerabilities.
  - Respond to intrusions.
- The Certifications emphasize 6 of the 11 job responsibility areas:
  - Analyze security incidents.
  - Assess and manage risk.
  - Communicate results.
  - Identify and mitigate vulnerabilities.
  - Log security incidents.
  - Manage security operations.
- The Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2) framework emphasizes 4 of the 11 job responsibility areas:
  - Assess and manage risk.
  - Communicate results.
  - Manage process and procedures.
  - Manage security operations.
- The Courses included emphasize 4 of the 11 job responsibility areas:
  - Assess and manage risk.
  - Identify and mitigate vulnerabilities.
  - Implement security monitoring.
  - Manage security operations.

- Two of the 11 job responsibility areas were not emphasized by any of the included programs:
  - Develop and manage personnel.
  - Manage projects and budgets.

The values in Table E.1 show the degree to which the listed program emphasizes the job responsibility area. These results are standardized, so the value of the number provides an understanding of the degree to which a program emphasizes the job responsibility area. A positive value (shaded green) shows the degree to which the job responsibility area is emphasized and a negative value (shaded red) shows the degree to which there is a lack of emphasis.

**Table E.1.** Overall Results of Workforce Program Emphasis of Responsibility Areas

Responsibility Area	Workforce Program				Comments
	NICE	Certifications	ES-C2M2	Courses	
Analyze security incidents	3.291	4.072	-1.018	-1.396	Two of the four programs emphasize analyzing security incidents, with Certifications showing the greatest emphasis.
Assess and manage risk	2.452	3.340	2.065	3.210	All four programs strongly emphasize assessing and managing risk, with Certifications showing the greatest emphasis.
Communicate results	2.905	2.570	1.866	-0.833	Three of the four programs emphasize communicating results, with NICE showing the greatest emphasis. Courses do not emphasize communicating results.
Develop and manage personnel	-0.280	-1.507	-1.632	-0.743	None of the programs emphasize developing and managing personnel.
Identify and mitigate vulnerabilities	2.677	2.234	-1.183	3.354	Three of the four programs emphasize identifying and mitigating vulnerabilities, with Courses showing the greatest emphasis. ES-C2M2 does not emphasize identifying and mitigating risks.
Implement security monitoring	-1.124	-1.470	-0.763	2.228	Only Courses emphasize implementing security monitoring.
Log security incidents	-1.635	2.677	-0.882	-1.569	Only Certifications emphasize logging security incidents.
Manage process and procedures	-1.367	-1.667	3.689	-1.306	Only ES-C2M2 emphasizes managing processes and procedures.
Manage projects and budgets	-0.413	-0.711	-1.234	-0.299	None of the programs emphasize managing projects and budgets.
Manage security operations	-1.638	2.431	3.346	2.222	Three of the four programs emphasize managing security operations, with ES-C2M2 showing the greatest emphasis. NICE does not emphasize managing security operations.
Respond to intrusions	2.470	-1.069	-0.878	-0.946	Only NICE emphasizes responding to intrusions.

## E.1 Differences between Panel and Public Results

While the table above shows the results of the votes of all participants, this section shows where the results from the public review (received through the RaCS) differed from the results of the SGC panel participants. Of the 44 possible mappings of whether a workforce program emphasizes a job responsibility area (shown above in Table E.1), the SGC panel and public participants differed on six of these alignments. Because the number of public participants was significantly greater than the number of SGC panel participants, in the overall results the areas of disagreement will tend to skew toward the public responses. The six areas of disagreement between the SGC panel and the public participants are shown in Table E.2.

**Table E.2.** Differences between SGC Panel and Public RaCS Results

Program	Job Responsibility Area	SGC Panel	RaCS Public	All Results
NICE	Manage security operations	2.229 (D)	-1.284	-1.638
Certifications	Identify and mitigate vulnerabilities	2.277	-2.097	2.234
	Manage security operations	-1.527	2.884	2.431
ES-C2M2	Develop and manage personnel	-1.710	1.548	-1.632
Courses	Analyze security incidents	2.079	-0.860	-1.396
	Log security incidents	2.135 (D)	-1.116	-1.569

(D) – indicates where panel members showed a lack of consensus (Dissensus)

## E.2 Analysis of Panel and Public Responses to RaCS to determine the Gaps and Overlaps (Alignment) in Cybersecurity Workforce Programs

Each of the charts below compares two workforce programs in terms of the responsibility areas that are emphasized (positive value), or that lack emphasis (negative value), in the listed workforce program. Respondents are filtered by “circles” as SGC Panel, RaCS Public, or Unfiltered for all respondents combined. The color of each cell is determined by the degree of agreement among the respondents by calculating a G-index (Holley and Lienert 1974) that is appropriate for assessing agreement among binary ratings for items in multiple, nonexclusive categories by an unequal number of raters. The interpretation of agreement indices (otherwise known as *Kappa* scores) is provided by Landis and Koch (1977). In accordance with their interpretation, the scores are highlighted in a color to indicate the level of agreement among the raters as shown in Table E.3 below.

**Table E.3.** Interpretation of Kappa Values

Level of Agreement	Interpretation	Color
<0.20	Poor to slight agreement	Red
0.21 – 0.60	Fair to moderate agreement	Orange
0.61 – 1.00	Substantial to perfect agreement	Green

The values shown for each responsibility area/workforce program are standardized z-scores indicating the relative degree to which raters indicated the responsibility area was included in the workforce

program detailed descriptors on a standardized scale from -5 to +5. For instance, in the case of the NICE Framework, the score indicates the relative number of NICE tasks that related to the listed responsibility area.

Positive	3 (Misalignment)	4 (Alignment)
Negative	1 (Gaps)	2 (Misalignment)
	Negative	Positive

**Figure E.1.** Gap/Alignment Quad Chart

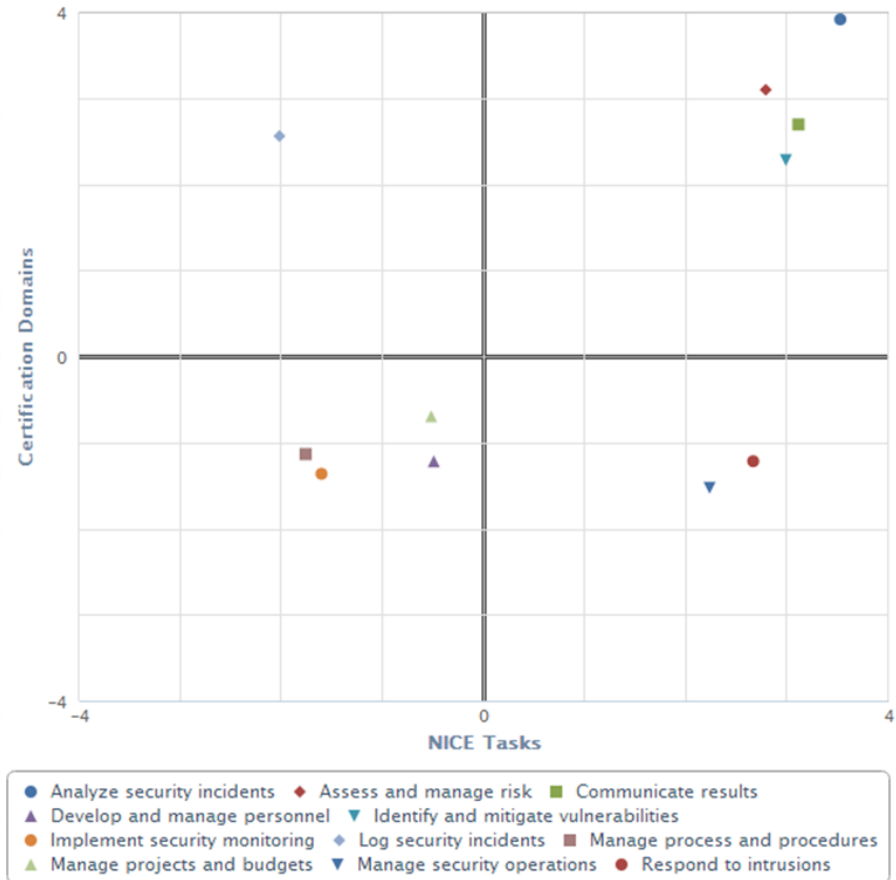
In the accompanying quadrant chart (Figure E.1), scaled to actual score values, the four cells correspond to the degree to which the z-scores were positive or negative. Thus, as shown in Figure E.1, four cells may be numbered based on the degree of gap (lack of emphasis), misalignment (one program emphasizes the responsibility while the other does not), and alignment (common emphasis) on each of the responsibility areas as follows:

- Quad 1 (lower left cell): Gaps – both programs lack an emphasis on the responsibility area.
- Quad 2 (lower right cell): Misalignment – program listed on left *emphasizes* a responsibility area that is not emphasized by the program listed on the right.
- Quad 3 (upper left cell): Misalignment – program listed on left *lacks emphasis* on a responsibility area that is emphasized by the program listed on the right.
- Quad 4 (upper right cell): Alignment – both programs emphasize the importance of the responsibility area.

The following sections include each of the comparative analyses for the panel respondents (first group), public respondents (second group), and overall response (third group), followed by a summary analysis. The final report will include the detailed analyses in an appendix while the focus of the findings section will be on the summary analysis.

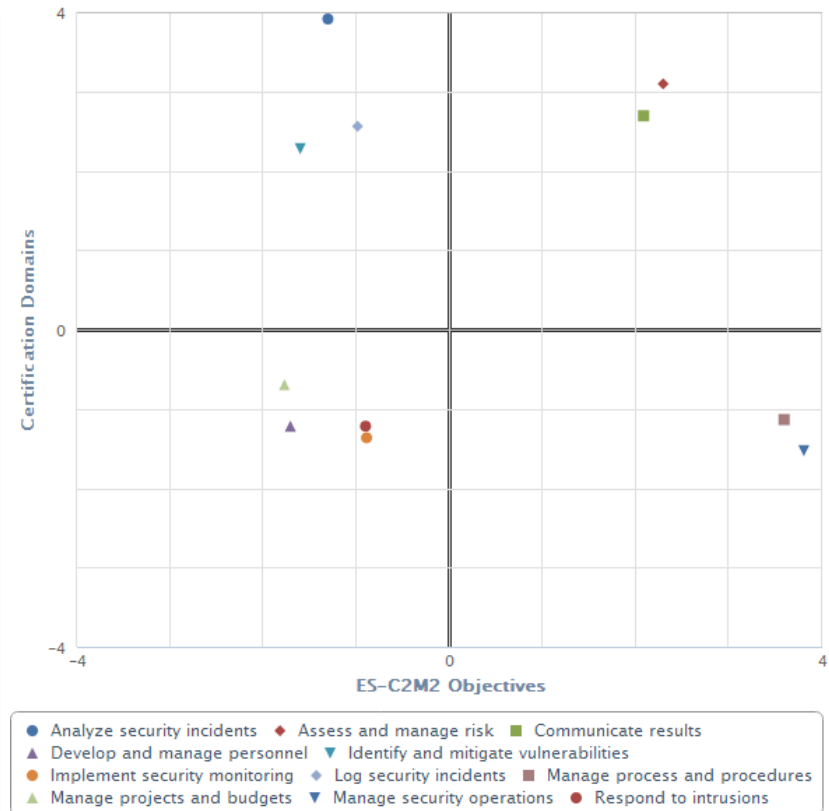
### E.3 Responses from the SGC Panel

	NICE Tasks	Certification Domains
<b>Quadrant 4: Alignment</b>		
Analyze security incidents	3.521	3.912
Assess and manage risk	2.784	3.095
Communicate results	3.107	2.693
Identify and mitigate vulnerabilities	2.983	2.277
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Log security incidents	-2.022	2.559
Manage security operations	2.229	-1.527
Respond to intrusions	2.660	-1.219
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-0.497	-1.219
Implement security monitoring	-1.607	-1.366
Manage process and procedures	-1.765	-1.139
Manage projects and budgets	-0.522	-0.697



**Figure E.2.** Responsibility Areas for NICE Tasks and Certifications. Filtered by Circle: SGC Panel

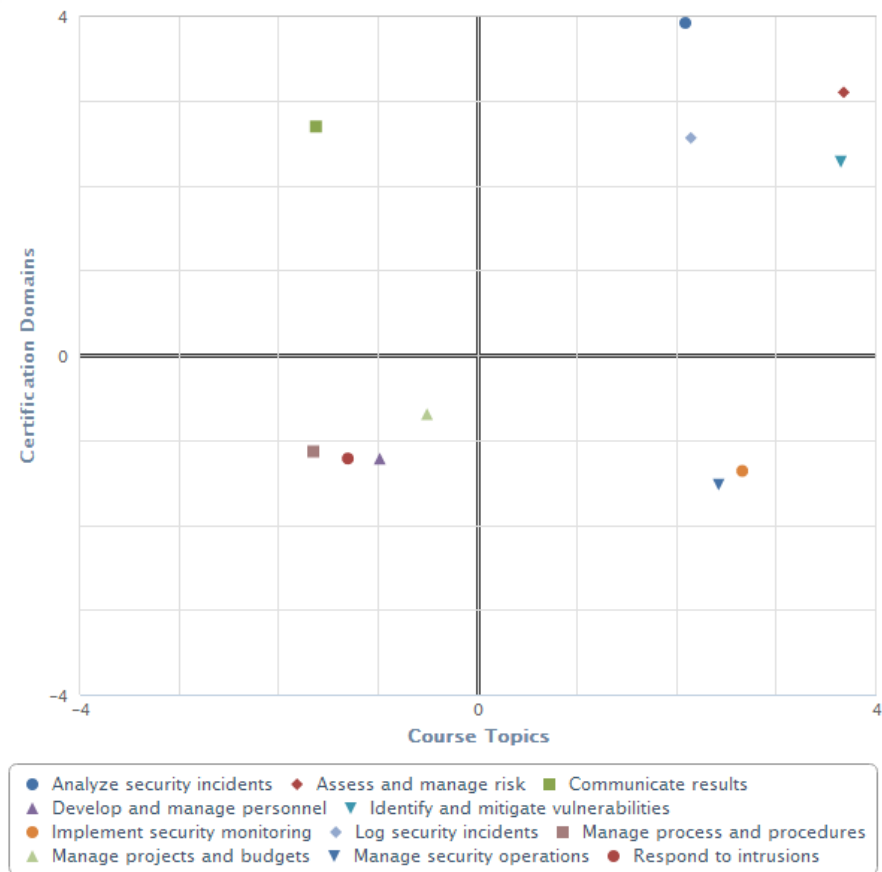
	ES-C2M2 Objectives	Certification Domains
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	2.294	3.095
Communicate results	2.082	2.693
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Analyze security incidents	-1.307	3.912
Identify and mitigate vulnerabilities	-1.604	2.277
Log security incidents	-0.988	2.559
Manage process and procedures	3.590	-1.139
Manage security operations	3.803	-1.527
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-1.710	-1.219
Implement security monitoring	-0.892	-1.366
Manage projects and budgets	-1.774	-0.697
Respond to intrusions	-0.903	-1.219



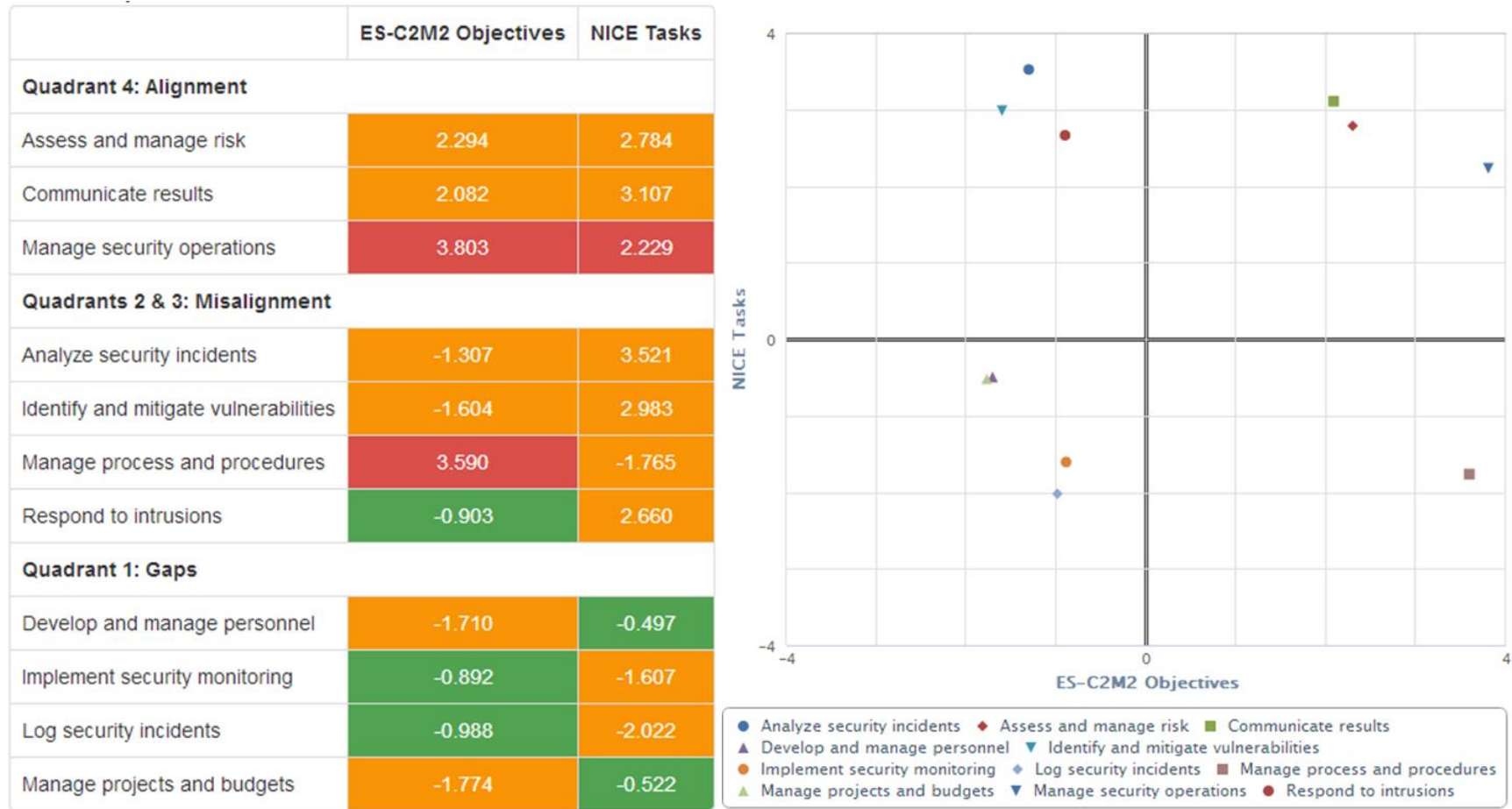
**Figure E.3.** Responsibility Areas for ES-C2M2 Objectives and Certifications. Filtered by Circle: SGC Panel



	Course Topics	Certification Domains
<b>Quadrant 4: Alignment</b>		
Analyze security incidents	2.079	3.912
Assess and manage risk	3.669	3.095
Identify and mitigate vulnerabilities	3.641	2.277
Log security incidents	2.135	2.559
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Communicate results	-1.632	2.693
Implement security monitoring	2.651	-1.366
Manage security operations	2.414	-1.527
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-0.991	-1.219
Manage process and procedures	-1.660	-1.139
Manage projects and budgets	-0.516	-0.697
Respond to intrusions	-1.311	-1.219

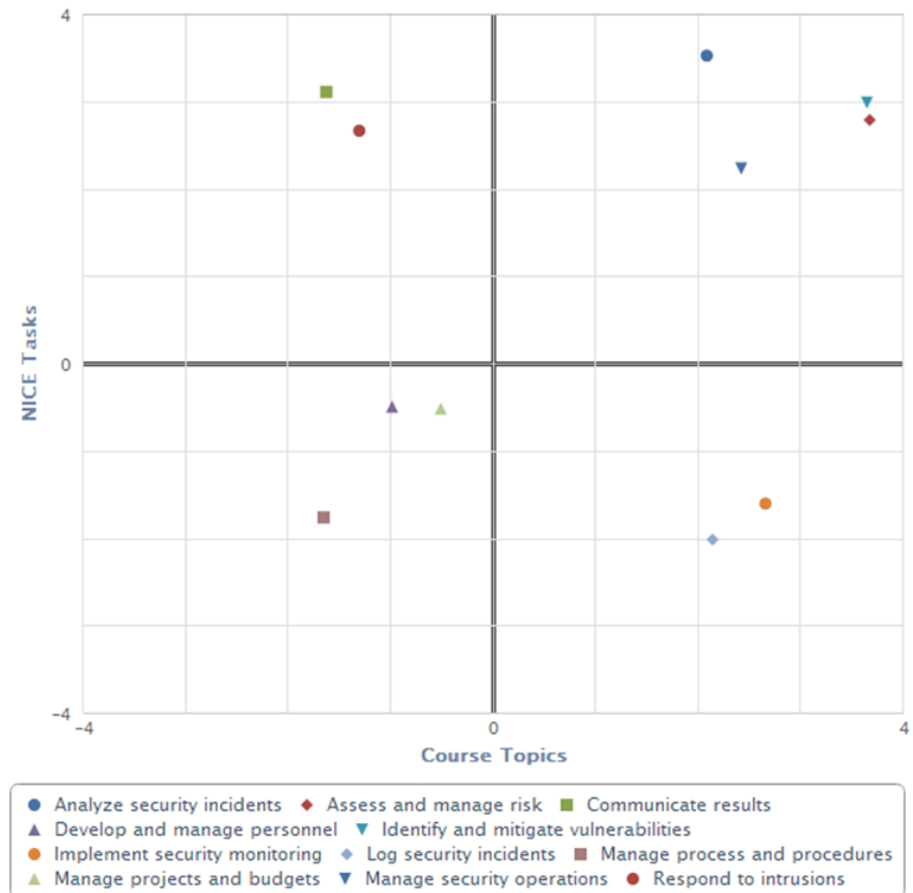


**Figure E.4.** Responsibility Areas for Course Topics and Certifications. Filtered by Circle: SGC Panel



**Figure E.5.** Responsibility Areas for C2M2 Objectives and NICE Tasks. Filtered by Circle: SGC Panel

	Course Topics	NICE Tasks
<b>Quadrant 4: Alignment</b>		
Analyze security incidents	2.079	3.521
Assess and manage risk	3.669	2.784
Identify and mitigate vulnerabilities	3.641	2.983
Manage security operations	2.414	2.229
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Communicate results	-1.632	3.107
Implement security monitoring	2.651	-1.607
Log security incidents	2.135	-2.022
Respond to intrusions	-1.311	2.660
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-0.991	-0.497
Manage process and procedures	-1.660	-1.765
Manage projects and budgets	-0.516	-0.522



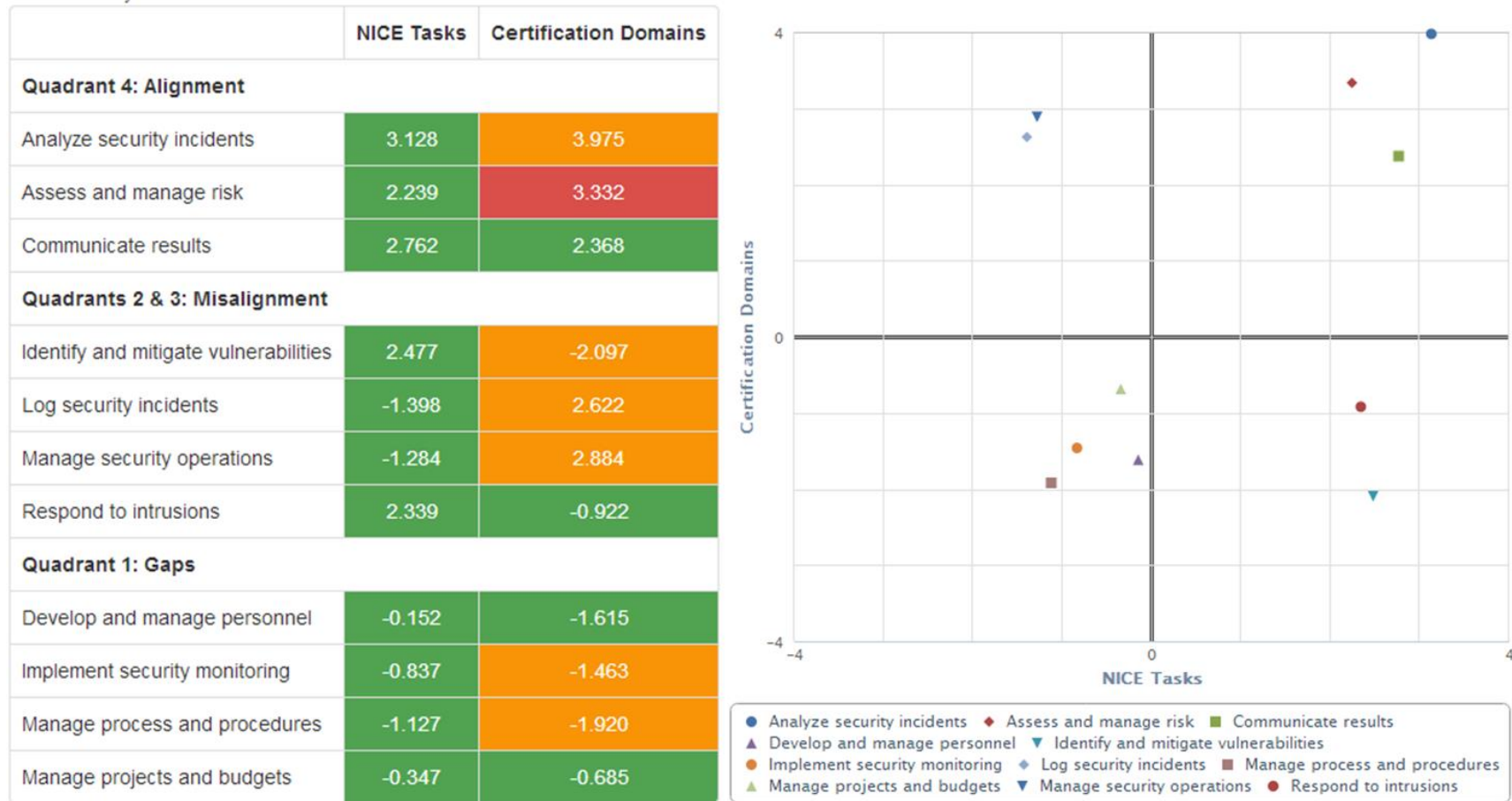
**Figure E.6.** Responsibility Areas for Course Topics and NICE Tasks. Filtered by Circle: SGC Panel

	ES-C2M2 Objectives	Course Topics
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	2.294	3.669
Manage security operations	3.803	2.414
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Analyze security incidents	-1.307	2.079
Communicate results	2.082	-1.632
Identify and mitigate vulnerabilities	-1.604	3.641
Implement security monitoring	-0.892	2.651
Log security incidents	-0.988	2.135
Manage process and procedures	3.590	-1.660
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-1.710	-0.991
Manage projects and budgets	-1.774	-0.516
Respond to intrusions	-0.903	-1.311



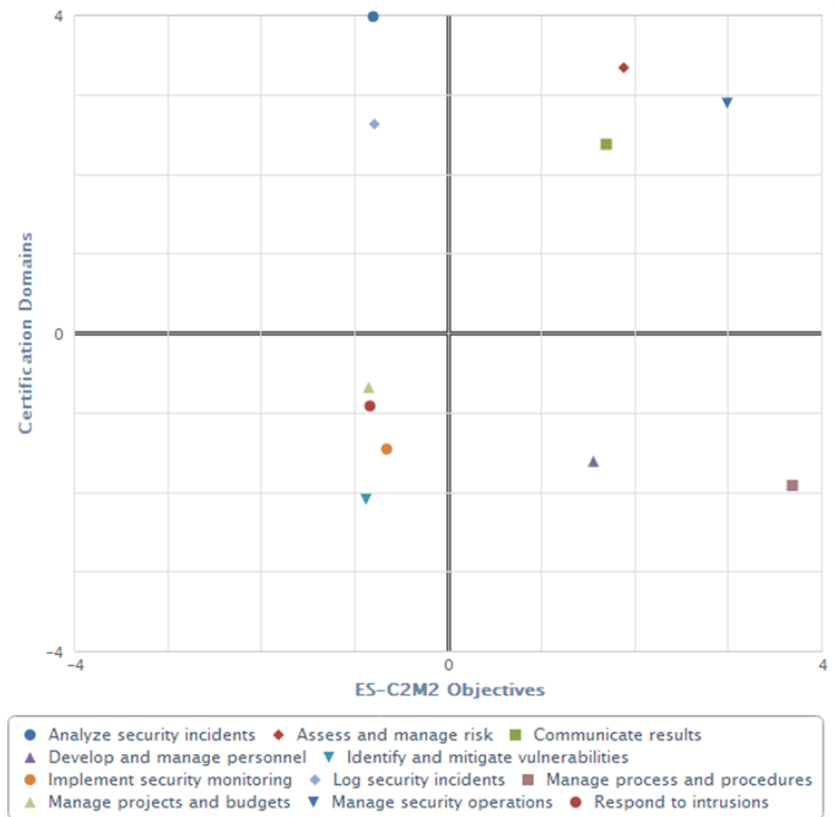
**Figure E.7.** Responsibility Areas for C2M2 Objectives and Course Topics. Filtered by Circle: SGC Panel

## E.4 Responses from the RaCS



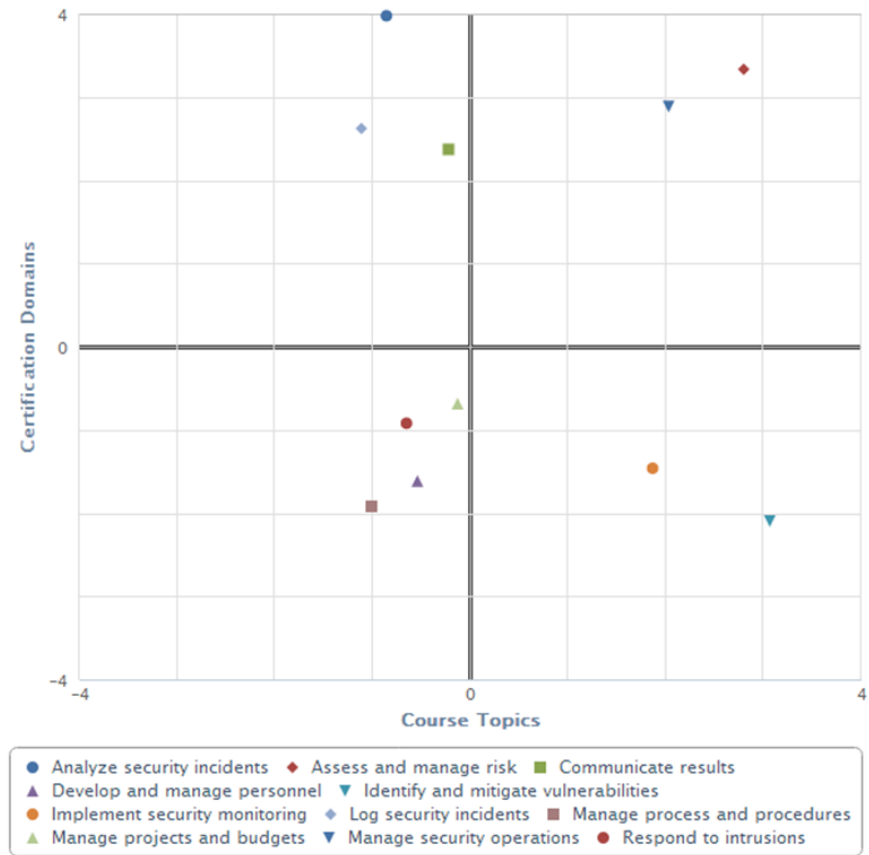
**Figure E.8.** Responsibility Areas for Nice Tasks and Certifications. Filtered by Circle: RaCS Public

	ES-C2M2 Objectives	Certification Domains
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	1.873	3.332
Communicate results	1.686	2.368
Manage security operations	2.979	2.884
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Analyze security incidents	-0.809	3.975
Develop and manage personnel	1.548	-1.615
Log security incidents	-0.795	2.622
Manage process and procedures	3.677	-1.920
<b>Quadrant 1: Gaps</b>		
Identify and mitigate vulnerabilities	-0.885	-2.097
Implement security monitoring	-0.664	-1.463
Manage projects and budgets	-0.857	-0.685
Respond to intrusions	-0.843	-0.922



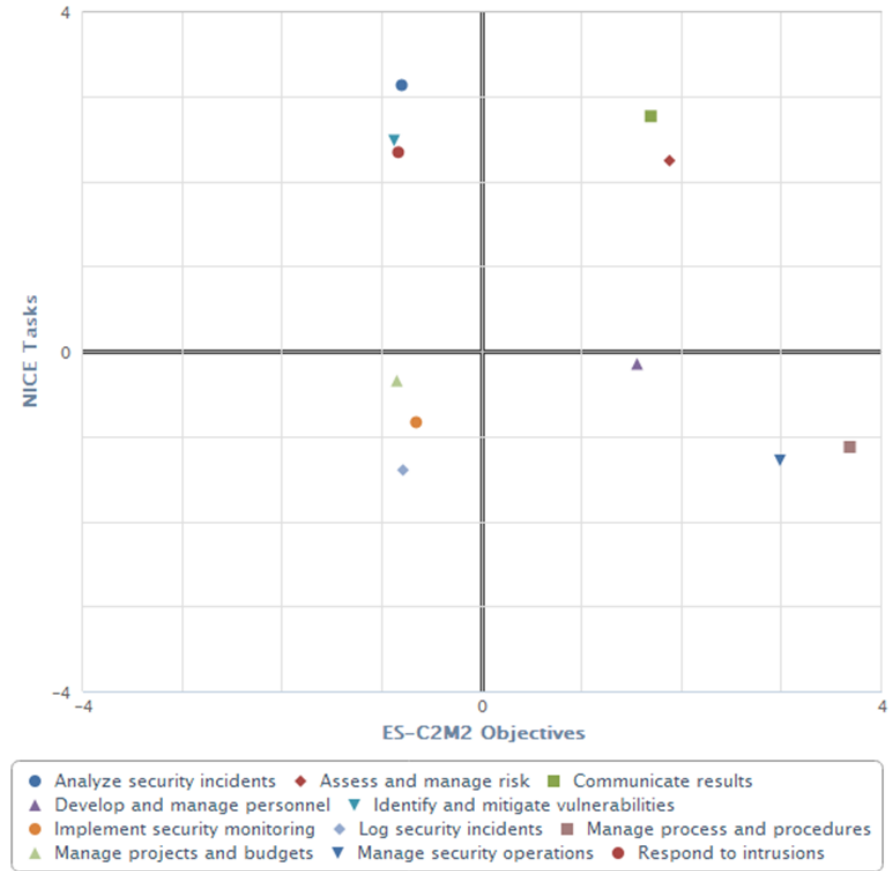
**Figure E.9.** Responsibility Areas for C2M2 Objectives and Certifications. Filtered by Circle: RaCS Public

	Course Topics	Certification Domains
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	2.795	3.332
Manage security operations	2.027	2.884
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Analyze security incidents	-0.860	3.975
Communicate results	-0.225	2.368
Identify and mitigate vulnerabilities	3.061	-2.097
Implement security monitoring	1.863	-1.463
Log security incidents	-1.116	2.622
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-0.543	-1.615
Manage process and procedures	-1.014	-1.920
Manage projects and budgets	-0.133	-0.685
Respond to intrusions	-0.655	-0.922



**Figure E.10.** Responsibility Areas for Course Topics and Certifications. Filtered by Circle: RaCS Public

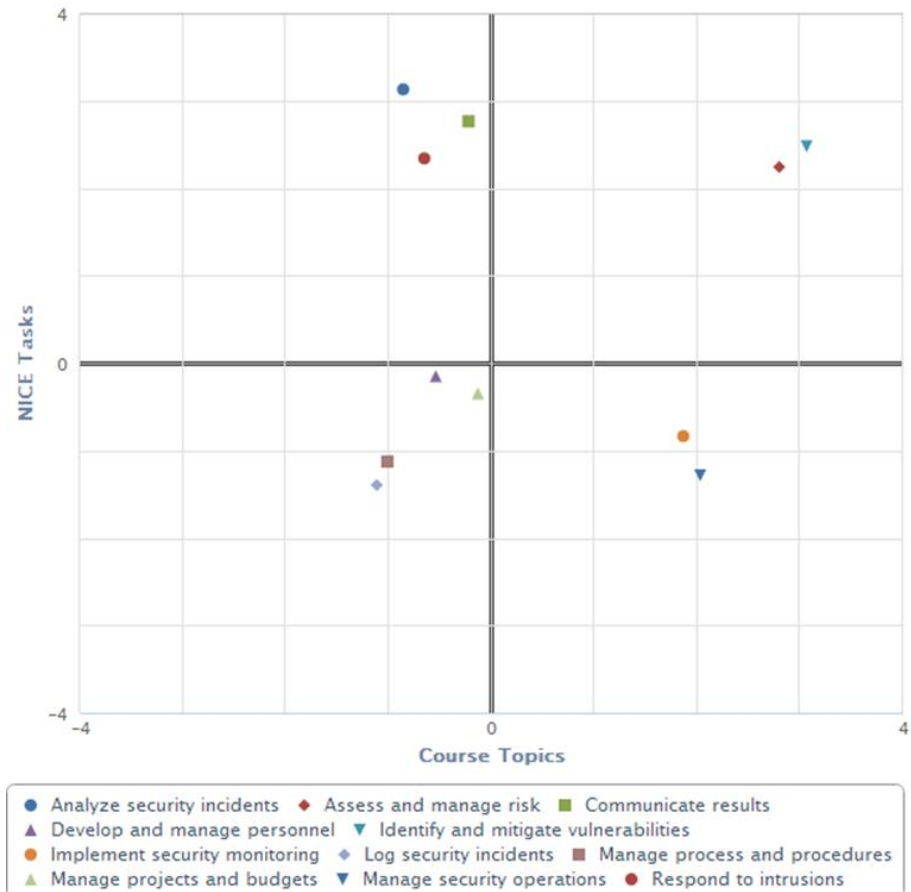
	ES-C2M2 Objectives	NICE Tasks
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	1.873	2.239
Communicate results	1.686	2.762
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Analyze security incidents	-0.809	3.128
Develop and manage personnel	1.548	-0.152
Identify and mitigate vulnerabilities	-0.885	2.477
Manage process and procedures	3.677	-1.127
Manage security operations	2.979	-1.284
Respond to intrusions	-0.843	2.339
<b>Quadrant 1: Gaps</b>		
Implement security monitoring	-0.664	-0.837
Log security incidents	-0.795	-1.398
Manage projects and budgets	-0.857	-0.347



**Figure E.11.** Responsibility Areas for C2M2 Objectives and NICE Tasks. Filtered by Circle: RaCS Public

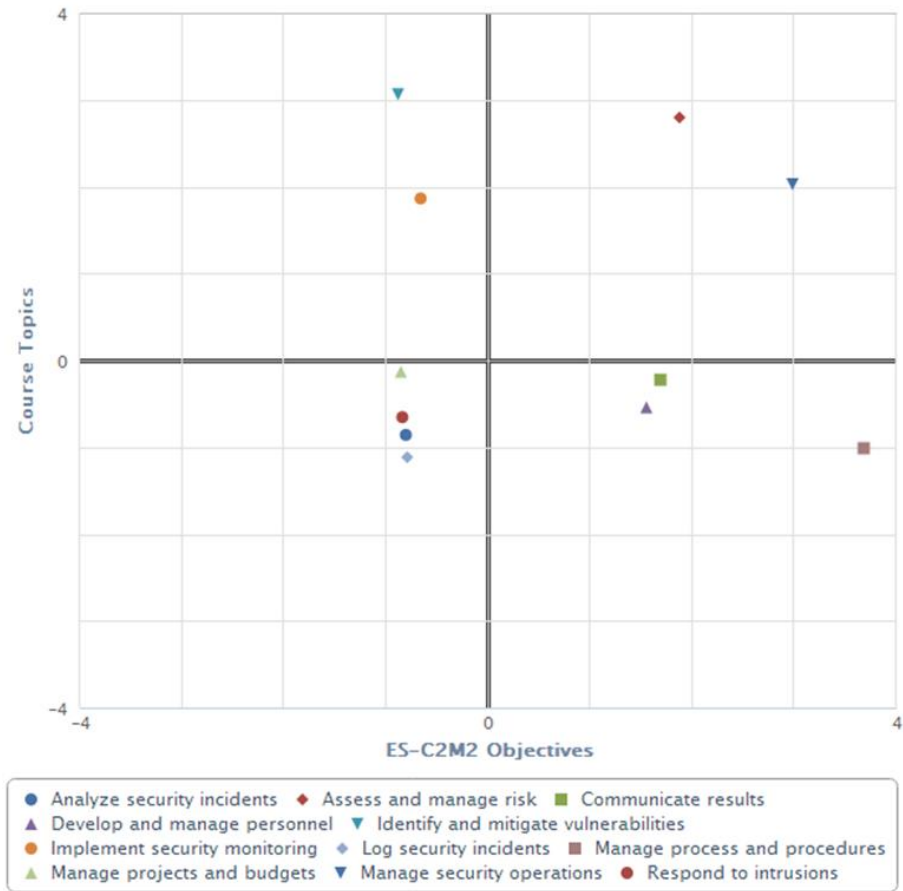


	Course Topics	NICE Tasks
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	2.795	2.239
Identify and mitigate vulnerabilities	3.061	2.477
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Analyze security incidents	-0.860	3.128
Communicate results	-0.225	2.762
Implement security monitoring	1.863	-0.837
Manage security operations	2.027	-1.284
Respond to intrusions	-0.655	2.339
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-0.543	-0.152
Log security incidents	-1.116	-1.398
Manage process and procedures	-1.014	-1.127
Manage projects and budgets	-0.133	-0.347



**Figure E.12.** Responsibility Areas for Course Topics and NICE Tasks. Filtered by Circle: RaCS Public

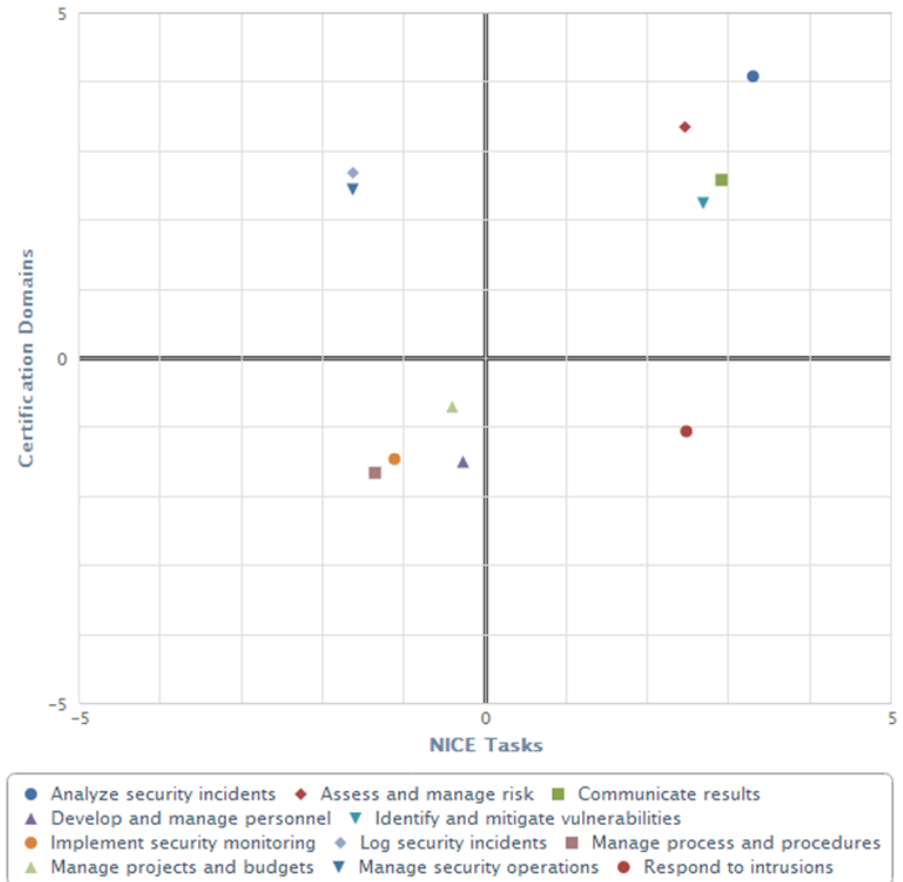
	ES-C2M2 Objectives	Course Topics
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	1.873	2.795
Manage security operations	2.979	2.027
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Communicate results	1.686	-0.225
Develop and manage personnel	1.548	-0.543
Identify and mitigate vulnerabilities	-0.885	3.061
Implement security monitoring	-0.664	1.863
Manage process and procedures	3.677	-1.014
<b>Quadrant 1: Gaps</b>		
Analyze security incidents	-0.809	-0.860
Log security incidents	-0.795	-1.116
Manage projects and budgets	-0.857	-0.133
Respond to intrusions	-0.843	-0.655



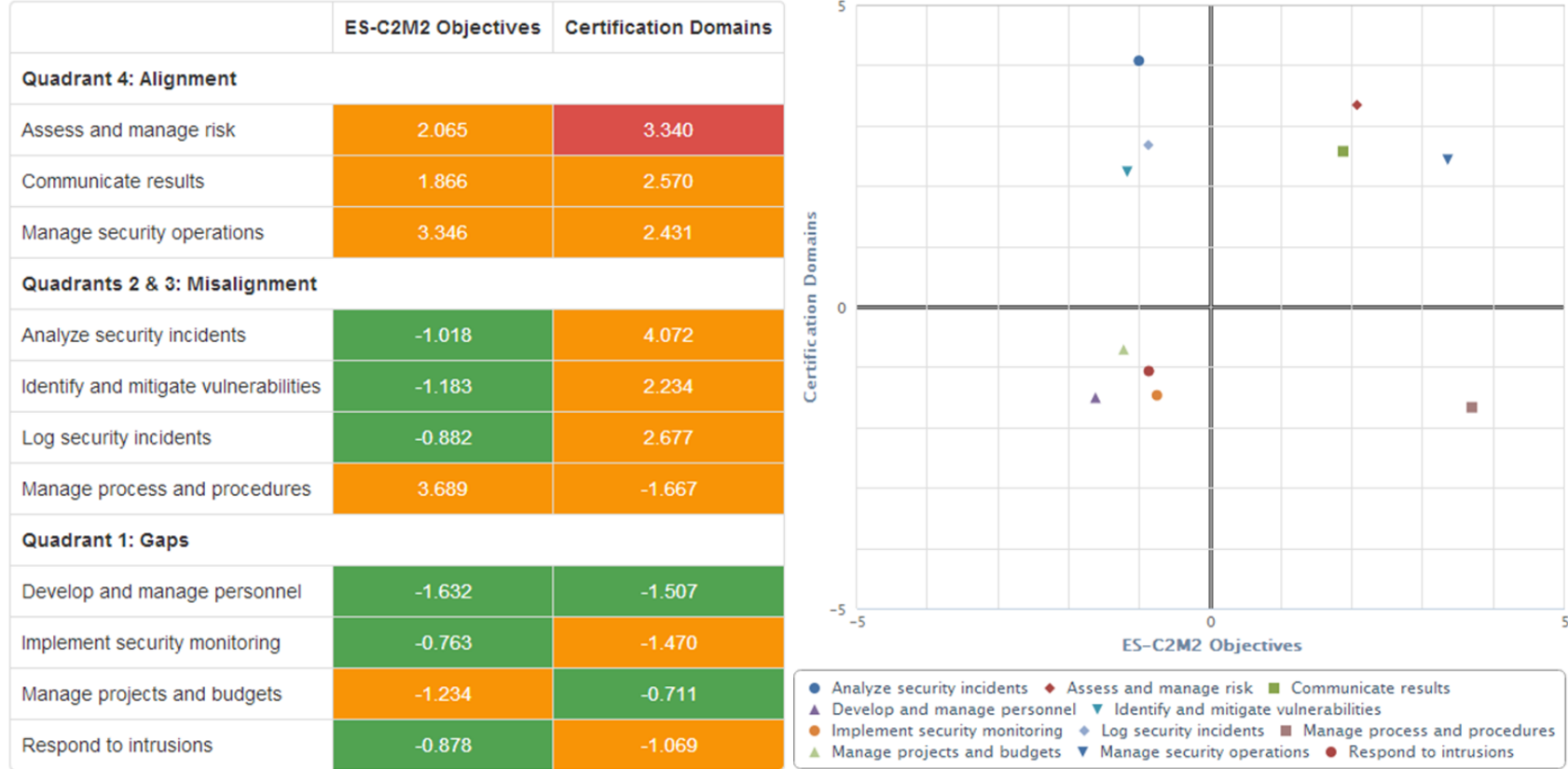
**Figure E.13.** Responsibility Areas for C2M2 Objectives and Course Topics. Filtered by Circle: RaCS Public

## E.5 All Responses Combined (Not Filtered)

	NICE Tasks	Certification Domains
<b>Quadrant 4: Alignment</b>		
Analyze security incidents	3.291	4.072
Assess and manage risk	2.452	3.340
Communicate results	2.905	2.570
Identify and mitigate vulnerabilities	2.677	2.234
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Log security incidents	-1.635	2.677
Manage security operations	-1.638	2.431
Respond to intrusions	2.470	-1.069
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-0.280	-1.507
Implement security monitoring	-1.124	-1.470
Manage process and procedures	-1.367	-1.667
Manage projects and budgets	-0.413	-0.711

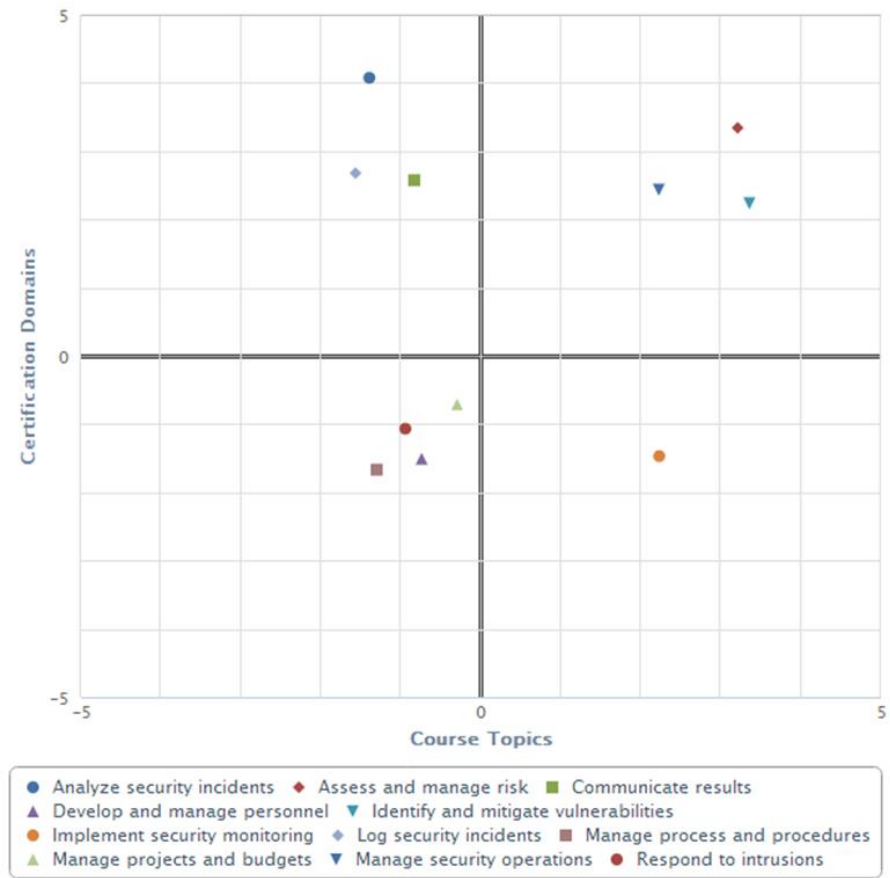


**Figure E.14.** Responsibility Areas for Nice Tasks and Certifications. Filtered by Circle: Not Filtered



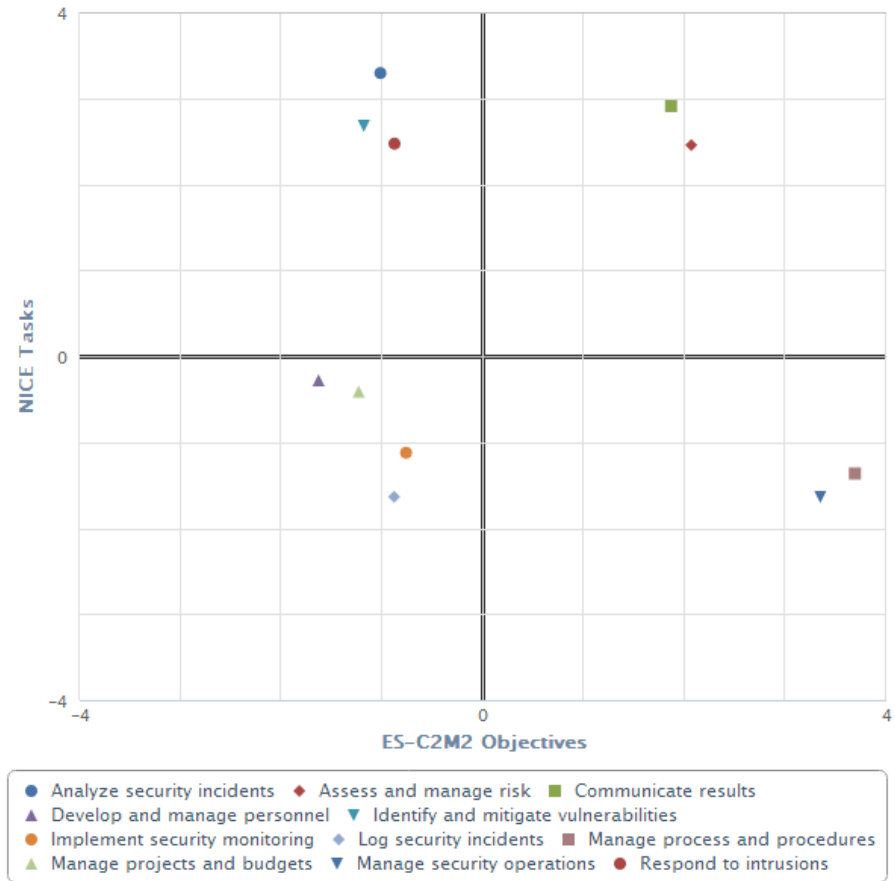
**Figure E.15.** Responsibility Areas for C2M2 Objectives and Certifications. Filtered by Circle: Not Filtered

	Course Topics	Certification Domains
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	3.210	3.340
Identify and mitigate vulnerabilities	3.354	2.234
Manage security operations	2.222	2.431
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Analyze security incidents	-1.396	4.072
Communicate results	-0.833	2.570
Implement security monitoring	2.228	-1.470
Log security incidents	-1.569	2.677
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-0.743	-1.507
Manage process and procedures	-1.306	-1.667
Manage projects and budgets	-0.299	-0.711
Respond to intrusions	-0.946	-1.069



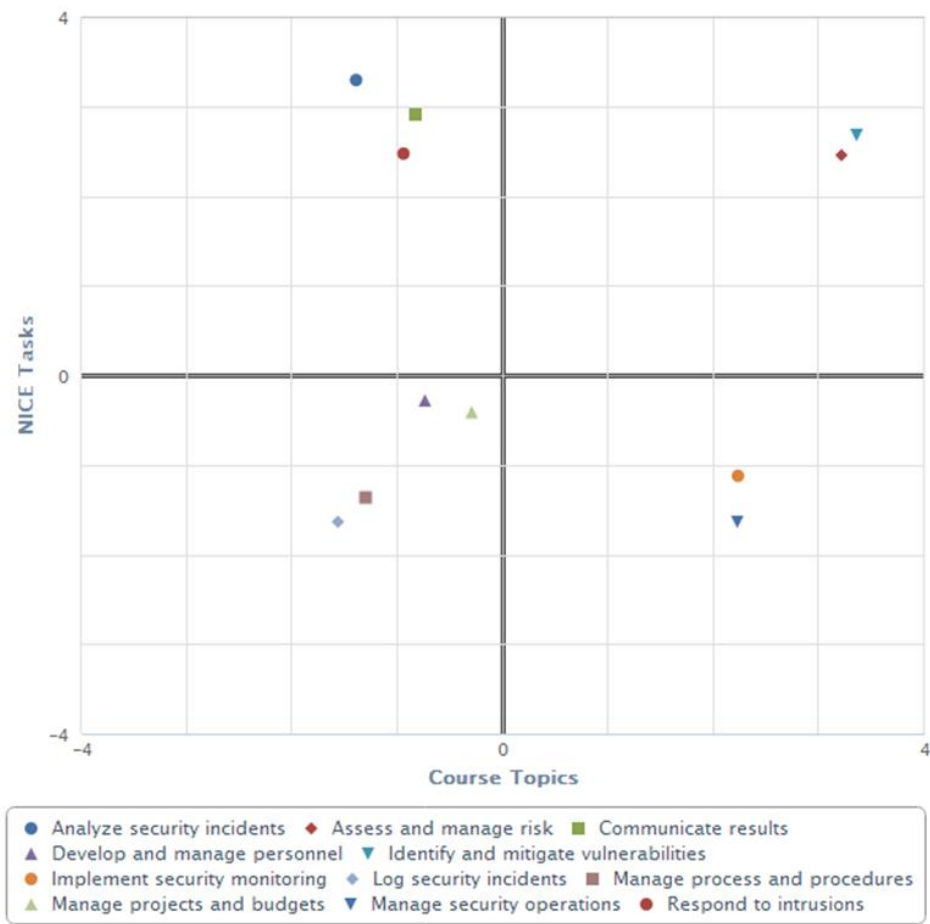
**Figure E.16.** Responsibility Areas for Course Topics and Certifications. Filtered by Circle: Not Filtered

	ES-C2M2 Objectives	NICE Tasks
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	2.065	2.452
Communicate results	1.866	2.905
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Analyze security incidents	-1.018	3.291
Identify and mitigate vulnerabilities	-1.183	2.677
Manage process and procedures	3.689	-1.367
Manage security operations	3.346	-1.638
Respond to intrusions	-0.878	2.470
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-1.632	-0.280
Implement security monitoring	-0.763	-1.124
Log security incidents	-0.882	-1.635
Manage projects and budgets	-1.234	-0.413



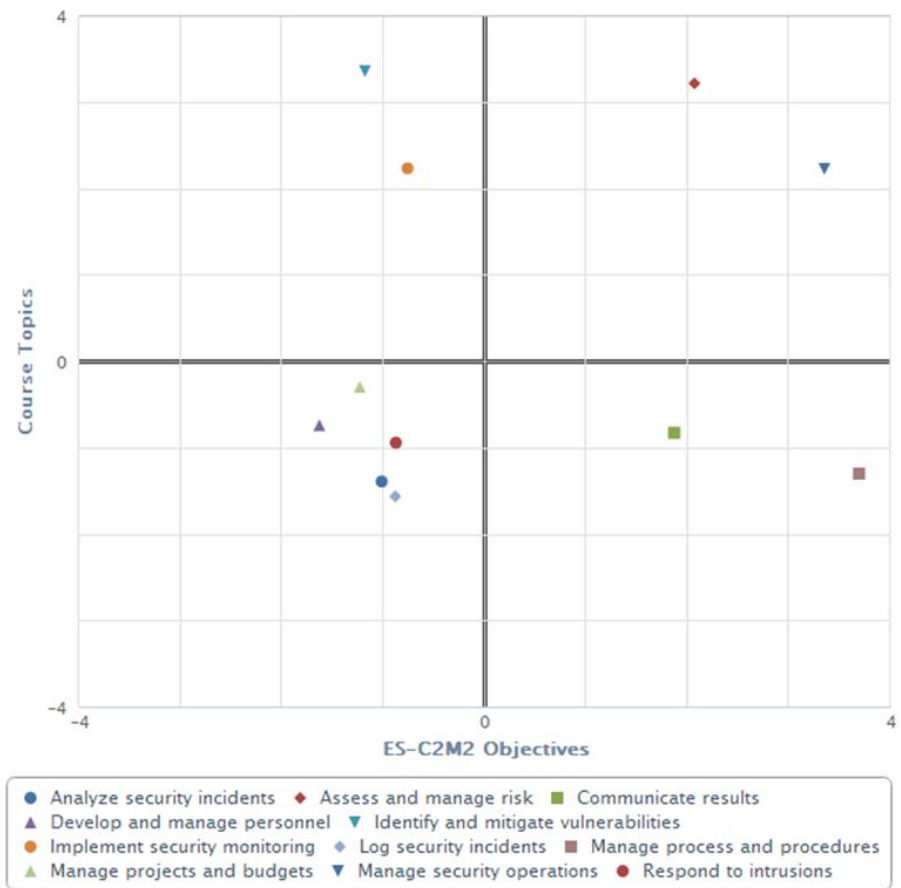
**Figure E.17.** Responsibility Areas for C2M2 Objectives and NICE Tasks. Filtered by Circle: Not Filtered

	Course Topics	NICE Tasks
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	3.210	2.452
Identify and mitigate vulnerabilities	3.354	2.677
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Analyze security incidents	-1.396	3.291
Communicate results	-0.833	2.905
Implement security monitoring	2.228	-1.124
Manage security operations	2.222	-1.638
Respond to intrusions	-0.946	2.470
<b>Quadrant 1: Gaps</b>		
Develop and manage personnel	-0.743	-0.280
Log security incidents	-1.569	-1.635
Manage process and procedures	-1.306	-1.367
Manage projects and budgets	-0.299	-0.413



**Figure E.18.** Responsibility Areas for Course Topics and NICE Tasks. Filtered by Circle: Not Filtered

	ES-C2M2 Objectives	Course Topics
<b>Quadrant 4: Alignment</b>		
Assess and manage risk	2.065	3.210
Manage security operations	3.346	2.222
<b>Quadrants 2 &amp; 3: Misalignment</b>		
Communicate results	1.866	-0.833
Identify and mitigate vulnerabilities	-1.183	3.354
Implement security monitoring	-0.763	2.228
Manage process and procedures	3.689	-1.306
<b>Quadrant 1: Gaps</b>		
Analyze security incidents	-1.018	-1.396
Develop and manage personnel	-1.632	-0.743
Log security incidents	-0.882	-1.569
Manage projects and budgets	-1.234	-0.299
Respond to intrusions	-0.878	-0.946



**Figure E.19.** Responsibility Areas for C2M2 Objectives and Course Topics. Filtered by Circle: Not Filtered



## E.6 References

- Holley JW and GA Lienert. 1974. "The G Index of Agreement in Multiple Ratings." *Educational and Psychological Measurement*, 34(4), 817–822. doi:10.1177/001316447403400409
- Landis JR and GG Koch. 1977. "The Measurement of Observer Agreement for Categorical Data." *Biometrics* 33, 159–174.



## **Appendix F**

### **Inter-Rater Reliability for SPSP Phase 2**



## Appendix F

### Inter-Rater Reliability for SPSP Phase 2

The Fleiss' Kappa measure was used to determine the amount of agreement that the raters (users) have in determining what certifications and what responsibilities are necessary for each job. There were 14 raters, 4 job roles (Intrusion Analysis, Security Operations, Cyber Secure Power Engineer, and Incident Response), 65 certifications, and 71 job responsibilities.

**Table F.1.** Certification Analyses Results

<b>Measure</b>	<b>Intrusion Analysis</b>	<b>Security Operations</b>	<b>Cyber Secure Power Engineer</b>	<b>Incident Response</b>
Fleiss' Kappa	0.1356	0.0617	0.1095	0.0739
p-value	<0.0001	0.0006	<0.0001	<0.0001
Interpretation	Agreement	Agreement	Agreement	Agreement

**Table F.2.** Job Responsibilities Analyses Results

<b>Measure</b>	<b>Intrusion Analysis</b>	<b>Security Operations</b>	<b>Cyber Secure Power Engineer</b>	<b>Incident Response</b>
Fleiss' Kappa	0.0987	0.0195	0.0165	0.1982
p-value	<0.0001	0.225	0.6530	<0.0001
Interpretation	Agreement	No Agreement	No Agreement	Agreement

The Fleiss' Kappa measure varies from just under 0 to 1, with larger values meaning more agreement. The p-value is the statistical probability that the null hypothesis ("No Agreement" or Fleiss' Kappa = 0) is true. In this case, p-values above 0.01 (alpha) were viewed as not rejecting the null ("No Agreement"), and p-values less than 0.01 were viewed as indicating some degree of agreement (statistically speaking). Table F.1 shows the inter-rater reliability measures for each job role across the many certifications. Table F.2 shows the inter-rater reliability measures for each job role across the many job responsibilities.

Data collected during a second session with the SGC panel investigated which learning objectives were associated with which responsibilities, as identified by 13 raters. The Fleiss' Kappa measure was used to determine the amount of agreement that the raters (users) have in determining which learning objectives are associated with each responsibility. There were 33 responsibilities included in the analysis and 25 of them (76%) had inter-rater reliability ratings that showed significant agreement. Eight of the responsibilities did not show agreement between the raters. The listing of each set of responsibilities can be found in Table F.3.

**Table F.3. Inter-Rater Results for Each Responsibility across Learning Objectives**

<b>Significant Inter-Rater Agreement</b>	<b>No Significant Inter-Rater Agreement</b>
Ensure a baseline of normal/expected activity is available or can be quickly assembled to support analysis	Ensure all appropriate parties are consulted and support security tool implementation
Ensure all data and evidence associated with intrusions is stored in an appropriate manner	Ensure all functional requirements meet current needs and identify tools that fall short
Ensure all incidents are classified into categories and provide data back to stakeholders; management; and risk assessment process	Ensure all security operations staff and stakeholders maintain an understanding of applicable vulnerabilities and threats
Ensure all intrusions are contained properly	Ensure all solutions being installed have been authorized
Ensure all intrusions are eradicated or cleaned to the greatest extent possible	Ensure Incident response and recovery procedures are tested regularly
Ensure all open intrusions are managed in a timely manner	Ensure only authorized staff can access security tools and data
Ensure all security events have been identified	Ensure the incident response procedure/plan is executed and followed
Ensure all security incident reporting requirements are satisfied properly	Ensure hardening of operating system; services; and applications on custom or third-party solutions
Ensure all security information regarding exposure; threats; protective measures is provided to develop appropriate risk picture	
Ensure incident data is collected; analyzed; maintained; and reviewed	
Ensure intrusions are closed by verifying incident response actions and testing targeted environment for additional attacker activity	
Ensure incident response (IR) Specialist has been trained and current in latest threats analysis	
Ensure logging and security information is stored for analysis for an appropriate period of time	
Ensure maintenance of security profiles for smart grid components	
Ensure maintenance of an accurate picture of utility systems deployed; architectures; communication protocols employed and business functions and processes	
Ensure monitoring of security state of your organization's systems and assets. Control access by applying the following concepts/methodologies/techniques: policies; types of controls; techniques; identification and authentication; decentralized/distributed access control techniques; authorization mechanisms; logging and monitoring	
Ensure operational security staff maintains a current understanding of Attack and Defense tactics, techniques and procedures (TTPs)	
Ensure security tools are patched and updated properly	
Ensure Security Information and Event Management system is operating to expected functional and/or performance requirements	
Ensure that personnel responsible for investigating security events understand what constitutes an actual event	
Ensure that security event types have been defined by classification; for example, an unauthorized access attempt to a firewall may not be considered an incident unless it meets a certain threshold (five attempts to the firewall may not be an incident; but 5000 attempts from the same IP address may be an indication of a denial-of-service attack)	
Ensure that you are receiving notifications from vendors in the case where they have been breached and maintain access to your networks	
Ensure the organization maintains an attack technique table with detailed TTPs	
Ensure you understand application, operating system and infrastructure to identify which tools best mitigate business risks	
Ensure false positives are tracked; provide advice for future filtering and close ticket	

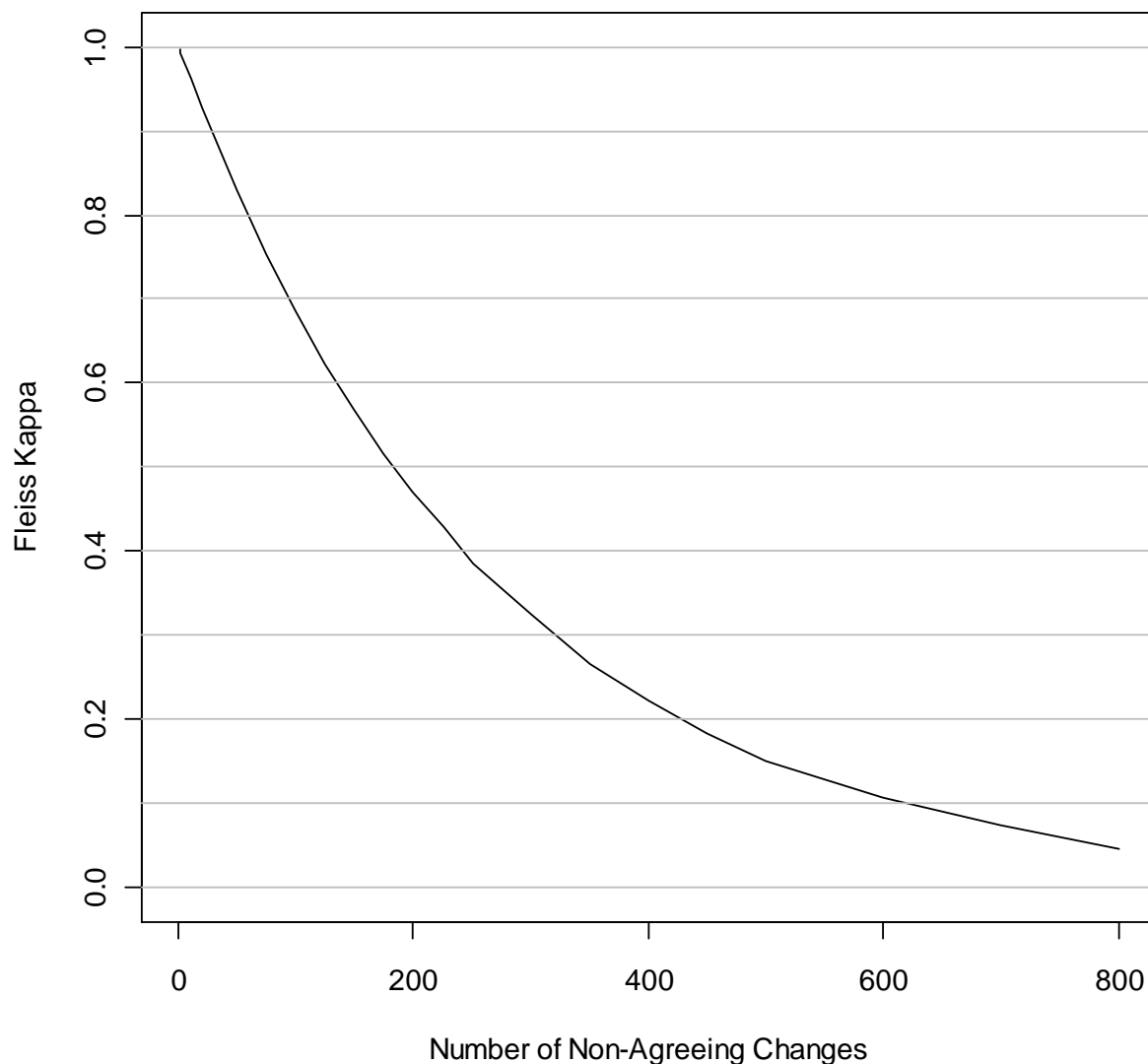
The fourth session with the SGC panel collected data concerning 11 responsibility areas and the three categories of C2M2 Objectives, Course Topics, and NICE tasks. Fleiss' Kappa measures were calculated for the raters concerning each responsibility area across each of the three categories. These results can be found in Table F.4. It is interesting to note that raters were not in agreement when classifying the

responsibility of “Manage security operations” for all three categories. “Develop and manage personnel” and “Manage projects and budgets” were also not in agreement for two of the three categories.

**Table F.4.** Inter-Rater Agreement for Responsibility Areas across C2M2 Objectives, Course Topics, and NICE Tasks

Significant Inter-Rater Agreement	No Significant Inter-Rater Agreement
<b>C2M2 Objectives</b>	
Analyze security incidents Assess and manage risk Communicate results Develop and manage personnel Identify and mitigate vulnerabilities Implement security monitoring Log security incidents Manage process and procedures Respond to intrusions	Manage projects and budgets Manage security operations
<b>Course Topics</b>	
Analyze security incidents Assess and manage risk Identify and mitigate vulnerabilities Implement security monitoring Log security incidents Manage process and procedures Respond to intrusions	Communicate results Develop and manage personnel Manage projects and budgets Manage security operations
<b>NICE Tasks</b>	
Analyze security incidents Assess and manage risk Communicate results Identify and mitigate vulnerabilities Implement security monitoring Log security incidents Manage process and procedures Manage projects and budgets Respond to intrusions	Develop and manage personnel Manage security operations

Interpreting the Fleiss’ Kappa values is difficult and the values are expected to be smaller as more categories (certifications and responsibilities) and more raters are included. The research team created a simulation to see whether it would help in understanding the Fleiss’ Kappa measures we had. The team created a dataset in perfect agreement (each rater agreed for each of the categories). This matrix was  $71 \times 15$ , meaning there were 1065 cells. Then the team simulated what the Fleiss’ Kappa value would be if one value (cell) was randomly changed, then two, and so on up to 800. The team ran 100 simulations at each of the number of values changed, and then calculated the average Fleiss’ Kappa value at each. The result is shown in Figure F.1 below.



**Figure F.1.** Simulation Results of the Number of Non-Agreeing Changes versus Fleiss Kappa Value

In conclusion, there was statistical agreement among the raters concerning certifications for each of the job roles. Intrusion Analysis had the most agreement, which according to the simulation would have been consistent with making over 500 changes from full agreement (just over half of the cells).

There was statistical agreement among the raters concerning job responsibilities for Intrusion Analysis and Incident Response. Incident Response had the most agreement, which according to the simulation would have been consistent with making just under 500 changes from full agreement (just under half of the cells). There was no statistical agreement between the raters for Security Operations and Cyber Secure Power Engineer.



## **Appendix G**

### **Knowledge Areas and Understanding Demonstrated for Each Certification**



## Appendix G

### Knowledge Areas and Understanding Demonstrated for Each Certification

**Table G.1.** Certified Information Systems Security Professional (CISSP)

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
Access Control	Control access by applying the following concepts/methodologies/techniques: (policies, types of controls, techniques, identification and authentication, decentralized/distributed access control techniques, authorization mechanisms, logging and monitoring)
	Understand access control attacks
	Assess effectiveness of access controls
	Identify and access provisioning lifecycles (e.g., provisioning, review, revocation)
Telecommunications and Network Security	Understand secure network architecture and design (e.g., Internet Protocol (IP) and non-IP protocols, segmentation)
	Securing network components
	Establish secure communications channels (e.g., virtual private network [VPN], Transport Layer Security/Secure Sockets Layer [TLS/SSL], virtual local area network [VLAN])
	Understand network attacks (e.g., distributed denial-of-service (DDoS), spoofing)
Information Security Governance and Risk Management	Understand and align security function to goals, mission and objectives of the organization
	Understand and apply security governance
	Understand and apply concepts of confidentiality, integrity, and availability
	Develop and implement security policy
	Manage the information life cycle (e.g., classification, categorization, and ownership)
	Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)
	Understand and apply risk management concepts
	Manage personnel security
	Develop and manage security education, training and awareness
	Manage the Security Function
Software Development Security	Understand and apply security in the software development cycle
	Understand the environment and security controls
	Assess the effectiveness of software security
Cryptography	Understand the application and use of cryptography
	Understand the cryptographic life cycle (e.g., cryptographic limitations, algorithm/protocol governance)
	Understand encryption concepts
	Understand key management processes
	Understand digital signatures
	Understand non-repudiation
	Understand methods of cryptanalytic attacks
	Use cryptography to maintain network security
	Use cryptography to maintain application security
	Understand public key infrastructure (PKI)

Knowledge Area	Understanding Demonstrated
Security Architecture and Design	Understand certificate related issues
	Understand information hiding alternatives (e.g., steganography, watermarking)
	Understand the fundamental concepts of security models (e.g., confidentiality, integrity, and multilevel models)
	Understand the components of information systems security evaluation models
	Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module)
	Understand the vulnerabilities of security architectures
	Understand software and system vulnerabilities and threats
	Understand countermeasure principles (e.g., defense in depth)
Operations Security	Understand security operations concepts
	Employ resource protection
	Manage incident response
	Implement preventative measures against attacks (e.g., malicious code, zero-day exploit, denial of service)
	Implement and support patch and vulnerability management
	Understand change and configuration management (e.g., versioning, base lining)
	Understand system resilience and fault tolerance requirements
Business Continuity and Disaster Recovery Planning	Understand business continuity requirements
	Conduct business impact analysis
	Develop a recovery strategy
	Understand a recovery strategy
	Understand disaster recovery process
	Exercise, assess and maintain the plan (e.g., version control, distribution)
Legal, Regulations, Investigations and Compliance	Understand legal issues that pertain to information security internationally
	Understand professional ethics
	Understand and support investigations
	Understand forensic procedures
	Understand compliance requirements and procedures
	Ensure security in contractual agreements and procurement processes (e.g., cloud computing, outsourcing, vendor governance)
Physical (Environmental) Security	Understand site and facility design consideration
	Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)
	Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)
	Support the implementation and operation of facilities security (e.g., technology convergence)
	Support the protection and securing of equipment
	Understand personnel privacy and safety (e.g., duress, travel, monitoring)

**Table G.2. System Operator Certification (SOC)**

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
Resource and Demand Balancing	Adjust or re-dispatch generation to implement proposed transmission system/equipment outages
	Adjust generation and interchange schedules to ensure adequate reserves and regulating margins are maintained
	Suspend Automatic Generation Control (AGC) when required
	Dispatch reserves when requested by a member of the Reserve Sharing Group.
	Monitor internal loads and adjust generation as needed
	Operate AGC equipment and validate against all timeline data that affects AGC
	Provide notifications of generating unit status following a forced outage
	Monitor the adequacy of resource plans to meet obligations
	Manually calculate ACE
	Adjust both short-term and future forecasts using actual load data and correction factors
Emergency Preparedness and Operations	Analyze bulk system disturbances
	Analyze forced equipment outages
	Take action to permit re-synchronizing and reconnecting to the Interconnection
	Coordinate emergency actions with affected systems
	Coordinate restoration activities with affected entities
	Coordinate the re-synchronization of transmission at preplanned locations
	Coordinate voltage reduction as requested or directed
	Develop and execute corrective actions when equipment ratings or operating limits are exceeded
	Declare a system emergency
	Determine the need for manual load shedding to prevent imminent separation from the Interconnection, voltage collapse, or other adverse consequence
	Implement a plan for restoring the system to a safe operating condition following a forced outage
	Direct actions to return the system to a secure state following a major system disturbance
	Declare a NERC Energy Emergency Alert
	Direct balancing authorities to take actions to mitigate IROL
	Evaluate requests for emergency removal of equipment
	Take action to minimize cascading outages
	Take appropriate measures due to loss of control center functionality
	Request emergency assistance from neighboring systems for maintaining system reliability
	Shed load for system reliability
	Report disturbances to NERC and the DOE following established guidelines
	Reestablish required operating reserve levels as soon as possible following a contingency that results in operating reserve usage
	Respond to system emergencies and frequency deviations to meet local, regional, and NERC DCS requirements
	Prepare for a capacity emergency by: bringing on all available generation, postponing equipment maintenance, reducing load, initiating voltage reductions
	Maintain system connectivity to the interconnection to maximize reliability
	Take action to protect the system if reliability becomes endangered by remaining interconnected
	Report any disturbances or unusual occurrences suspected or determined to be caused by sabotage to the appropriate systems, governmental agencies, and regulatory bodies.
	Following a partial or total system shutdown, implement the appropriate provisions and procedures of the system's restoration plan in a coordinated

Knowledge Area	Understanding Demonstrated
	manner with adjacent systems, arrange for start-up and/or emergency power for generation units as required, arrange for and utilize emergency (backup) telecommunications facilities as required, restore the integrity of the Interconnection as soon as possible
	Monitor and periodically test normal and emergency telecommunication systems to ensure that communications are adequate and continuous
	Identify and take action when partial or full system islanding occurs
	Identify and take actions when a partial or full system voltage collapse occurs
	Following the activation of automatic load shedding schemes: restore system load as appropriate for current system conditions and in coordination with adjacent systems, shed additional load manually if there is insufficient generation to support the connected load, monitor system voltage levels to ensure high voltage conditions do not develop, monitor system frequency to ensure high frequency conditions do not develop, monitor the performance of any automatic load restoration relays, resynchronize transmission at preplanned locations if possible
	Utilize operating reserves to assist recovery of system frequency
	Obtain resources to restore system frequency
System Operations	Analyze generating unit outage requests to ensure system reliability
	Analyze transmission facility outage requests to ensure system reliability
	Analyze and respond to SCADA inputs (e.g., system voltage, line loading, and system alarms, etc.
	Communicate planned equipment outages to affected entities and Reliability Coordinators (RCs)
	Communicate forced outages and unusual system events to affected entities and RCs
	Comply with RC directives
	Coordinate the response to forced outages to ensure system reliability
	Coordinate next-day study model changes with RC Area Balancing Authorities (BAs)
	Coordinate planned transmission and generation outages with all impacted systems for system reliability
	Coordinate Reliability must run unit requirements
	Coordinate switching with affected systems
	Coordinate with adjacent BA on outage of tie-line metering
	Perform a contingency analysis for next-day scheduled outages
	Develop a contingency plan responding to equipment outages
	Monitor generating unit outputs during normal and abnormal conditions
	Develop operating plans based on the results of a contingency analysis
	Coordinate future study results for outage coordination
	Monitor system conditions to determine actual or potential threats to system reliability
	Evaluate the impact of current and forecast weather conditions on system operations
	Respond to conditions that may lead to voltage collapse
	Initiate hotline calls as appropriate to share reliability information
	Issue corrective actions to Balancing Authorities and Transmission Operators as required
	Maintain constant communications with all affected areas to ensure reliable and secure operation of the bulk electricity system
	Monitor actual or contingent system operating limit violations and respond as required
	Monitor and respond to telecommunication alarms or failures

Knowledge Area	Understanding Demonstrated
	Monitor Interconnection frequency and investigate causes of unexpected deviations
	Provide notifications for computer system hardware and software failure
	Respond to light load conditions
	Obtain power flow studies to identify ways to reconfigure the system for real-time and/or Real Time Contingency Analysis (RTCA) violations.
	Utilize State Estimator results to determine missing or erroneous telemetered data
	Obtain contingency case for scheduled outages for next-day operation
	Ensure all balancing authorities or transmission operators are aware of geomagnetic disturbances (GMD) forecast information.
	Monitor all reliability-related data within a reliability authority area
Interchange Scheduling and Coordination	Calculate inadvertent interchange
	Coordinate with adjacent entity as to actual and scheduled interchange values
	Perform checkout of daily and hourly scheduled and actual interchange
	Take action to minimize the impact of interchange schedules across constrained interfaces
	Monitor tagging system for new, revised, and adjusted interchange transactions
	Ensure the accuracy of hourly tie line readings
	Manually enter schedule interchange value due to system failure
	Manually enter telemetered tie line data due to signal failure with tie point
	Manually calculate net interchange
	Monitor status of NERC interchange transaction tags to ensure timely approval and implementation
	Protect the confidentiality of all interchange transaction information
	Curtail tags for reliability
	Ensure that the ramp rate, start and end times, energy profile, and losses are communicated to all parties in the transaction
	Reestablish curtailed interchange transactions with affected balancing authorities or transmission operators
Transmission Operations	Reconfigure the transmission system to implement proposed transmission system/equipment outages
	Call out system personnel for forced transmission outages
	Cancel scheduled transmission work when system conditions require
	Control transmission loading by reconfiguring the transmission system
	Direct and control transmission switching
	Direct the energizing of new facilities
	Approve requests for energizing new facilities
	Communicate equipment loading issues with Reliability Coordinator
	Monitor transmission line loading
	Authorize switching on clearances involving critical facilities.
	Provide notifications of transmission equipment status following a forced outage
	Request line loading relief procedures
	Direct line loading relief procedures
	Adjust transfers across interfaces or paths to maintain system reliability
	Perform reliability analysis to determine impact of: scheduled outages, forced outages
Protection and Control	Analyze the impact of protection equipment outages on system reliability
	Ensure special protective systems and remedial action schemes are enabled when needed for system reliability
	Maintain adequate protective relaying during all phases of the system restoration
	Take action in response to alarms from special protective schemes

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
	Schedule system telecommunications, telemetering, protection, and control equipment outages to ensure system reliability
Voltage and Reactive	Monitor regional reactive reserve availability, including dynamic resources
	Monitor and maintain defined voltage profiles/limits to ensure system reliability
	Restore dynamic reactive reserves as soon as possible after use
	Utilize transmission line removal as a voltage control tool
	Monitor the status and availability of generator voltage regulators and/or power system stabilizers, and respond as required to deficiencies that may impact system reliability
	Coordinate operation of voltage control equipment with interconnected utilities
	Utilize reactive resources from transmission and generator owners to maintain acceptable voltage profiles
Interconnection Reliability Operations and Coordination	Monitor RC area and wide-area view of the bulk electricity system
	Perform next day reliability analysis
	Perform reliability assessment of all tags prior to implementation
	Re-dispatch generation as directed by the RC
	Direct generation re-dispatch to ensure transmission reliability limits are not violated
	Formulate a plan to implement corrective actions when an operating reliability limit violation is anticipated
	Obtain load-flow modeling tool results to determine power flow changes and optimum system configurations during normal and emergency conditions
	Monitor system frequency and initiate a hotline conference call when frequency error exceeds specific limits
	Perform next-day reliability analysis of the electricity system
	Notify all affected areas that line loading relief has been requested, and that corrective actions are required
	Coordinate reliability processes and actions with and among other reliability coordinators
	Identify, communicate, and direct actions to relieve reliability threats and limit violations in the reliability authority area
	Direct transmission and generator operators to revise maintenance plans as required, and as permitted by agreements
	Recalculate interconnection reliability operating limits based on current or future conditions, and according to transmission and generator owners' specified equipment ratings
	Review generation operations plans and commitments from balancing authorities for reliability assessment
	Review transmission maintenance plans from transmission operators for reliability assessment
	Direct transmission operators and balancing authorities to take actions to mitigate interconnection reliability operating limits (IROL)



**Table G.3. Certified Ethical Hacker (CEH)**

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
Introduction to Ethical Hacking	Understand the issues plaguing the information security world
	Gain knowledge on various hacking terminologies
	Learn the basic elements of information security
	Understand the security, functionality and ease of use triangle
	Know the five stages of ethical hacking
	Understand the different types and implications of hacker attacks
	Understand hactivism and understand the classification of hackers
	Understand who is an ethical hacker
	Gain information on how to become an ethical hacker
	Learn the profile of a typical ethical hacker
	Understand scope and limitations of ethical hacking
	Understand vulnerability research and list the various vulnerability research tools
	Learn the different ways an ethical hacker tests a target network
	Understand penetration testing and the various methodologies used
Footprinting and Reconnaissance	Understand the term Footprinting
	Learn the areas and information that hackers seek
	Gain knowledge on information gathering tools and methodology
	Understand the role of financial websites in footprinting
	Understand competitive intelligence and its need
	Understand DNS enumeration
	Understand Whois
	Learn different types of DNS records
	Understand how traceroute is used in Footprinting
	Recognize the role of search engines in footprinting
	Learn the website mirroring tools
	Understand how e-mail tracking works
	Understand Google hacking and its tools
	Learn the countermeasures to be taken in footprinting
Scanning Networks	Understand pen testing
	Understand the terms port scanning, network scanning and vulnerability scanning
	Understand the objectives of scanning
	Learn the CEH scanning methodology
	Understand Ping Sweep techniques
	Understand the Firewalk tool
	Gain knowledge on Nmap command switches
	Understand the three way handshake
	Learn TCP communication flag types
	Gain knowledge on War dialing techniques
	Understand banner grabbing using OS fingerprinting, active stack fingerprinting, passive fingerprinting and other techniques and tools
	Learn vulnerability scanning using BidiBlah and other hacking tools
	Learn to draw network diagrams of vulnerable hosts using various tools
	Understand how proxy servers are used in launching an attack
	Gain insights on working of anonymizers
	Identify HTTP tunneling techniques
	Identify IP spoofing techniques
	Understand various scanning countermeasures
Enumeration	Learn the system hacking cycle
	Understand Enumeration and its techniques

Knowledge Area	Understanding Demonstrated
	Understand null sessions and its countermeasures
	Understand SNMP enumeration and its countermeasures
	Describe the steps involved in performing enumeration
System Hacking	Understand the different types of passwords
	Identify the different types of password attacks
	Identify password cracking techniques
	Understand Microsoft authentication mechanism
	Describe password sniffing
	Identifying various password cracking tools
	Identify various password cracking countermeasures
	Understand privilege escalation
	Gain insights on key loggers and other spyware technologies
	Learn how to defend against spyware
	Identify different ways to hide files
	Understanding rootkits
	Learn how to identify rootkits and steps involved
	Understand Alternate Data Streams
	Understand steganography technologies and tools used
	Understand covering tracks, tools used and erase evidences
Trojans and Backdoors	Define a Trojan
	Identify overt and covert channels
	Understand working of Trojans
	Identify the different types of Trojans
	What do Trojan creators look for
	Identify the different ways a Trojan can infect a system
	How to indicate a Trojan attack
	Identify the ports used by Trojan
	Identify listening ports using netstat
	Understand “wrapping”
	Understand Reverse Shell Trojan
	Understand ICMP tunneling
	Identify various classic Trojans
	Learn windows start up monitoring tools
	Understand the Trojan horse constructing kit
	Learn Trojan detection techniques
	Learn Trojan evading techniques
	Learn how to avoid a Trojan infection
Viruses and Worms	Understand virus and its history
	Characteristics of a virus
	Learn the working of a virus
	Understand the motive behind writing a virus
	Understand how a computer becomes infected by viruses
	Gain insights on virus hoax
	Understand virus analysis
	Understand the difference between a virus and a worm
	Understand the life cycle of virus
	Identify the types of viruses
	Understand how a virus spreads and infects the system
	Understand the storage pattern of virus
	Identify various types of classic virus found in the wild
	Virus writing technique
	Virus construction kits

Knowledge Area	Understanding Demonstrated
	Understand antivirus evasion techniques
	Understand virus detection methods and countermeasures
	Understand worm analysis
Sniffers	Understand sniffing and protocols vulnerable to it
	Identify types of sniffing
	Understand Address Resolution Protocol (ARP)
	Understanding the process of ARP Spoofing
	Understand active and passive sniffing
	Understand ARP poisoning
	Understand MAC duplicating
	Learn ethereal capture and display filters
	Understand MAC flooding
	Understand DNS spoofing techniques
	Identify sniffing countermeasures
	Know various sniffing tools
	Identify sniffing detection and defensive techniques
Social Engineering	Understand social engineering
	Understand human weakness
	Identify the different types of social engineering
	Learn warning signs of an attack
	Understand Dumpster Diving
	Understand human-based social engineering
	Understand insider attacks and their countermeasures
	Gain insights on social engineering threats and defense
	Comprehend identity theft
	Understand phishing attacks
	Identify online scams
	Understand URL obfuscation
	Understand social engineering on social networking sites
	Identify social engineering countermeasures
Denial of Service	Understand a denial-of-service (DoS) attack
	Gain insights on distributed Denial of Service Attacks
	Examine the working of Distributed Denial of Service Attacks
	Analyze Symptoms of a DoS attack
	Understand Internet Chat Query (ICQ)
	Understand Internet Relay Chat (IRC)
	Assess DoS attack techniques
	Understand Botnets
	Assess DoS/DDoS attack tools
	Describe detection techniques
	Identify DoS/DDoS countermeasure strategies
	Analyze post-attack forensics
	Identify DoS/DDoS protection tools
	Understand DoS/DDoS penetration testing
Session Hijacking	Understand what session hijacking is
	Identify key session hijacking techniques
	Understand brute-force attack
	Understand HTTP referrer attack
	Spoofing vs. Hijacking
	Understand session hijacking process
	Identify types of session hijacking
	Analyze Session Hijacking in OSI Model

Knowledge Area	Understanding Demonstrated
	Understand application-level session hijacking
	Discuss session sniffing
	Describe man-in-the-middle attack
	Understand man-in-the-browser attack
	Examine steps to perform man-in-the-browser attack
	Understand client-side attacks
	Understand cross-site script attack
	Understand session fixation attack
	Describe network level session hijacking
	Understand TCP/IP hijacking
	Identify session hijacking tools
	Identify countermeasures for session hijacking
	Understand Session Hijacking Pen Testing
Hacking Webservers	Understand open- source Web server architecture
	Examine IIS Web server architecture
	Understand Website defacement
	Understand why Web servers are compromised
	Analyze impact of Web server attacks
	Examine Web server misconfiguration
	Understand Directory Traversal Attacks
	Learn regarding HTTP Response Splitting attack
	Understand Web Cache Poisoning attack
	Understand HTTP Response Hijacking
	Discuss SSH brute force attack
	Examine man-in-the-middle attack
	Learn Web server password cracking techniques
	Identify Web application attacks
	Understand Web server attack methodology
	Identify Web server attack tools
	Identify counter-measures against Web server attacks
	Understand patch management
	Assess Web server security tools
	Understand Web server Pen Testing
Hacking Web Applications	Understand Introduction to Web Applications
	Identify Web Application components
	Understand working of Web Applications
	Examine Web Application architecture
	Assess Parameter/Form Tampering
	Understand Injection Flaws
	Discuss hidden field manipulation attack
	Describe cross-site scripting (XSS) attacks
	Understand Web Services Attack
	Understand Web Application Hacking Methodology
	Identify Web Application Hacking Tools
	Understand how to defend against Web Application Attacks
	Identify Web Application security tools
	Understand Web Application firewalls
	Gain insights on Web Application Pen Testing
SQL Injection	Understand SQL Injection
	Examine SQL injection attacks
	Understand working of Web Applications
	Identify Server Side Technologies

Knowledge Area	Understanding Demonstrated
	Understand SQL Injection Detection
	Discuss SQL Injection Black Box Pen Testing
	Types of SQL Injection
	Understand blind SQL injection
	Learn SQL injection methodology
	Understand SQL query
	Examine Advanced Enumeration
	Describe password grabbing
	Discuss grabbing SQL server hashes
	Identify SQL injection tools
	Understand evasion techniques for SQL injection
	Understand defensive strategies against SQL injection attacks
	Identify SQL injection detection tools
Hacking Wireless Networks	Understand wireless networks
	Gain insights on wireless networks
	Understand various types of wireless networks
	Understand Wi-Fi authentication modes
	Identify types of wireless encryption
	Understand WEP Encryption
	Understand WPA/WPA2
	Discuss wireless threats
	Understand wireless hacking methodology
	Assess wireless hacking tools
	Understand Bluetooth hacking
	Understand how to defend against Bluetooth hacking
	Understand how to defend against wireless attacks
	Identify Wi-Fi security tools
	Examine wireless penetration testing framework
Evading IDS, Firewalls, and Honeypots	Understand intrusion detection systems (IDS)
	Learn ways to detect an intrusion
	Acquire knowledge on various types of intrusion detection systems
	Understand what is a Firewall
	Types of Firewall
	Identify firewall identification techniques
	Understand honeypots
	Assess various types of honeypot
	Understand how to set up a honeypot
	Understand IDS, firewall and honeypot systems
	Examine Evading IDS
	Understand Evading Firewall
	Learn detecting Honeypots
	Identify Firewall Evading tools
	Identify Countermeasures
	Analyze Firewall and IDS Penetration Testing
Buffer Overflow	Understand Buffer Overflows (BoF)
	Understand Stack-Based Buffer Overflow
	Know Heap-Based Buffer Overflow
	Understand Stack Operations
	Identify Buffer Overflow Steps
	Analyze attacking a Real Program
	Examine smashing the stack
	Examples of Buffer Overflow

Knowledge Area	Understanding Demonstrated
	Understand how to mutate a buffer overflow exploit
	Learn how to identify Buffer Overflows
	Testing for heap overflow conditions: heap.exe
	Understand steps for testing stack overflow in OllyDbg Debugger
	Identify Buffer overflow detection tools
	Understand defense against buffer overflows
	Identify Buffer Overflow countermeasures tools
	Understand Buffer Overflow pen testing
Cryptography	Understand cryptography
	Learn various types of cryptography
	Understand ciphers
	Gain insights on Advanced Encryption Standard (AES)
	Understand RC4, RC5, RC6 algorithms
	Examine RSA (Rivest Shamir Adleman)
	Explain Message Digest Function: MD5
	Understand Secure Hashing Algorithm (SHA)
	Identify cryptography tools
	Understand Public Key Infrastructure (PKI)
	Understand e-mail encryption
	Identify digital signature
	Describe SSL (Secure Sockets Layer)
	Examine disk encryption
	Identify disk encryption tools
	Understand cryptography attacks
	Identify cryptanalysis tools
Penetration Testing	Understand penetration testing (PT)
	Identify security assessments
	Examine risk management
	Understand various types of penetration testing
	Understand automated testing
	Understand manual testing
	Understand penetration testing techniques
	Know the penetration testing phases
	Understand enumerating devices
	Understand Penetration Testing Roadmap
	Understand Denial of Service Emulation
	Outsourcing pen testing Services
	Identify various Penetration testing tools

**Table G.4. Certified information Security Auditor (CISA)**

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
The Process of Auditing Information Systems	Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included.
	Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
	Conduct audits in accordance with IT audit standards to achieve planned audit objectives
	Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary
	Conduct follow-ups or prepare status reports to ensure appropriate actions have been taken by management in a timely manner
	Knowledge of ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards
	Knowledge of risk assessment concepts, tools and techniques in an audit context
	Knowledge of control objectives and controls related to information systems
	Knowledge of audit planning and audit project management techniques, including follow-up
	Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) including relevant IT
	Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation, and frequency of audits
	Knowledge of evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis) used to gather, protect and preserve audit evidence
	Knowledge of different sampling methodologies
	Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure)
	Knowledge of audit quality assurance systems and frameworks
Governance and Management of IT	Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives.
	Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
	Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.
	Evaluate the organization's IT policies, standards, and procedures, and the processes for their development, approval, implementation, maintenance, and monitoring, to determine whether they support the IT strategy and comply with regulatory and legal requirements.
	Evaluate the adequacy of the quality management system to determine whether it supports the organization's strategies and objectives in a cost-effective manner.
	Evaluate IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures
	Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives
	Evaluate IT contracting strategies and policies, and contract management practices to determine whether they support the organization's strategies and objectives

Knowledge Area	Understanding Demonstrated
	Evaluate risk management practices to determine whether the organization's IT-related risks are properly managed
	Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance
	Evaluate the organization's business continuity plan to determine the organization's ability to continue essential business operations during the period of an IT disruption
	Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines, and practices
	Knowledge of the purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each
	Knowledge of organizational structure, roles and responsibilities related to IT
	Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures
	Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions
	Knowledge of relevant laws, regulations and industry standards affecting the organization
	Knowledge of quality management systems
	Knowledge of the use of maturity models
	Knowledge of process optimization techniques
	Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, project management)
	Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes including third-party outsourcing relationships
	Knowledge of enterprise risk management
	Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators [KPI])
	Knowledge of IT human resources (personnel) management practices used to invoke the business continuity plan
	Knowledge of business impact analysis (BIA) related to business continuity planning
	Knowledge of the standards and procedures for the development and maintenance of the business continuity plan and testing methods
Information Systems Acquisition, Development, and Implementation	Evaluate the business case for the proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives
	Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization
	Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation, and status reporting is accurate
	Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements
	Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls and organization's requirements are met
	Conduct post-implementation reviews of systems to determine whether project deliverables, controls and organization's requirements are met



Knowledge Area	Understanding Demonstrated
	Knowledge of benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], return on investment [ROI])
	Knowledge of project governance mechanisms (e.g., steering committee, project oversight board, project management office)
	Knowledge of project management control frameworks, practices and tools
	Knowledge of risk management practices applied to projects
	Knowledge of IT architecture related to data, applications and technology (e.g., distributed applications, web-based applications, web services, n-tier applications)
	Knowledge of acquisition practices (e.g., evaluation of vendors, vendor management, escrow)
	Knowledge of requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis, vulnerability management, security requirements)
	Knowledge of project success criteria and risks
	Knowledge of control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data
	Knowledge of system development methodologies and tools including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques)
	Knowledge of testing methodologies and practices related to information systems development
	Knowledge of configuration and release management relating to the development of information systems
	Knowledge of system migration and infrastructure deployment practices and data conversion tools, techniques and procedures
	Knowledge of post-implementation review objectives and practices (e.g., project closure, control implementation, benefits realization, performance measurement)
Information Systems Operations, Maintenance and Support	Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives
	Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed
	Evaluate third-party management practices to determine whether the levels of controls expected by the organization are being adhered to by the provider
	Evaluate operations and end-user procedures to determine whether scheduled and nonscheduled processes are managed to completion
	Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the organization's objectives
	Evaluate data administration practices to determine the integrity and optimization of databases
	Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the organization's objectives
	Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner
	Evaluate change, configuration and release management practices to determine whether scheduled and nonscheduled changes made to the organization's production environment are adequately controlled and documented
	Evaluate the adequacy of backup and restore provisions to determine the availability of information required to resume processing
	Evaluate the organization's disaster recovery plan to determine whether it enables the recovery of IT processing capabilities in the event of a disaster

Knowledge Area	Understanding Demonstrated
	Knowledge of service level management practices and the components within a service level agreement
	Knowledge of techniques for monitoring third party compliance with the organization's internal controls
	Knowledge of operations and end-user procedures for managing scheduled and nonscheduled processes
	Knowledge of the technology concepts related to hardware and network components, system software and database management systems
	Knowledge of control techniques that ensure the integrity of system interfaces
	Knowledge of software licensing and inventory practices
	Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)
	Knowledge of database administration practices
	Knowledge of capacity planning and related monitoring tools and techniques
	Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)
	Knowledge of problem and incident management practices (e.g., help desk, escalation procedures, tracking)
	Knowledge of processes, for managing scheduled and nonscheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices
	Knowledge of data backup, storage, maintenance, retention and restoration practices
	Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery
	Knowledge of business impact analysis (BIA) related to disaster recovery planning
	Knowledge of the development and maintenance of disaster recovery plans
	Knowledge of types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites, cold sites)
	Knowledge of processes used to invoke the disaster recovery plans
	Knowledge of disaster recovery testing methods
Protection of Information Assets	Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices
	Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information
	Evaluate the design, implementation, and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures, and applicable external requirements
	Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded
	Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data, and softcopy media) to determine whether information assets are adequately safeguarded
	Knowledge of the techniques for the design, implementation, and monitoring of security controls, including security awareness programs
	Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)
	Knowledge of logical access controls for the identification, authentication and restriction of users to authorized functions and data
	Knowledge of the security controls related to hardware, system software (e.g.,

Knowledge Area	Understanding Demonstrated
	applications, operating systems), and database management systems
	Knowledge of risks and controls associated with virtualization of systems
	Knowledge of the configuration, implementation, operation and maintenance of network security controls
	Knowledge of network and Internet security devices, protocols, and techniques
	Knowledge of information system attack methods and techniques
	Knowledge of detection tools and control techniques (e.g., malware, virus detection, spyware)
	Knowledge of security testing techniques (e.g., intrusion testing, vulnerability scanning)
	Knowledge of risks and controls associated with data leakage
	Knowledge of encryption-related techniques
	Knowledge of public key infrastructure (PKI) components and digital signature techniques
	Knowledge of risks and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs)
	Knowledge of controls and risks associated with the use of mobile and wireless devices
	Knowledge of voice communications security (e.g., PBX, VoIP)
	Knowledge of the evidence preservation techniques and processes followed in forensics investigations (e.g., IT, process, chain of custody)
	Knowledge of data classification standards and supporting procedures
	Knowledge of physical access controls for the identification, authentication and restriction of users to authorized facilities
	Knowledge of environmental protection devices and supporting practices
	Know the processes and procedures used to store, retrieve, transport and dispose of confidential information assets

**Table G.5. Certified Information Security Manager (CISM)**

Knowledge Area	Understanding Demonstrated
Information Security Governance	Establish and maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program
	Establish and maintain an information security governance framework to guide activities that support the information security strategy
	Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program
	Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures and guidelines
	Develop business cases to support investments in information security
	Identify internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy
	Obtain commitment from senior management and support from other stakeholders to maximize the probability of successful implementation of the information security strategy
	Define and communicate the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of

Knowledge Area	Understanding Demonstrated
	authority
	Establish, monitor, evaluate and report metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy
	Knowledge of methods to develop an information security strategy
	Knowledge of the relationship among information security and business goals, objectives, functions, processes and practices
	Knowledge of methods to implement an information security governance framework
	Knowledge of the fundamental concepts of governance and how they relate to information security
	Knowledge of methods to integrate information security governance into corporate governance
	Knowledge of internationally recognized standards, frameworks and best practices related to information security governance and strategy development
	Knowledge of methods to develop information security policies
	Knowledge of methods to develop business cases
	Knowledge of strategic budgetary planning and reporting methods
	Knowledge of the internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) and how they impact the information security strategy
	Knowledge of methods to obtain commitment from senior management and support from other stakeholders for information security
	Knowledge of information security management roles and responsibilities
	Knowledge of organizational structures and lines of authority
	Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization
	Knowledge of methods to select, implement and interpret metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs])
Information Risk Management and Compliance	Establish and maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value
	Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels
	Ensure that risk assessments, vulnerability assessments and threat analyses are conducted periodically and consistently to identify risk to the organization's information
	Determine appropriate risk treatment options to manage risk to acceptable levels
	Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level
	Identify the gap between current and desired risk levels to manage risk to an acceptable level
	Integrate information risk management into business and IT processes (for example, development, procurement, project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the organization
	Monitor existing risk to ensure that changes are identified and managed appropriately
	Report noncompliance and other changes in information risk to appropriate management to assist in the risk management decision-making process
	Knowledge of methods to establish an information asset classification model consistent with business objectives

Knowledge Area	Understanding Demonstrated
	Knowledge of methods used to assign the responsibilities for and ownership of information assets and risk
	Knowledge of methods to evaluate the impact of adverse events on the business
	Knowledge of information asset valuation methodologies
	Knowledge of legal, regulatory, organizational and other requirements related to information security
	Knowledge of reputable, reliable and timely sources of information regarding emerging information security threats and vulnerabilities
	Knowledge of events that may require risk reassessments and changes to information security program elements
	Knowledge of information threats, vulnerabilities and exposures and their evolving nature
	Knowledge of risk assessment and analysis methodologies
	Knowledge of methods used to prioritize risk
	Knowledge of risk reporting requirements (for example, frequency, audience, components)
	Knowledge of methods used to monitor risk
	Knowledge of risk treatment strategies and methods to apply them
	Knowledge of control baseline modeling and its relationship to risk-based assessments
	Knowledge of information security controls and countermeasures and the methods to analyze their effectiveness and efficiency
	Knowledge of gap analysis techniques as related to information security
	Knowledge of techniques for integrating risk management into business and IT processes
	Knowledge of compliance reporting processes and requirements
	Knowledge of cost/benefit analysis to assess risk treatment options
Information Security Program Development and Management	Establish and maintain the information security program in alignment with the information security strategy
	Ensure alignment between the information security program and other business functions (for example, human resources [HR], accounting, procurement and IT) to support integration with business processes
	Identify, acquire, manage and define requirements for internal and external resources to execute the information security program
	Establish and maintain information security architectures (people, process, technology) to execute the information security program
	Establish, communicate and maintain organizational information security standards, procedures, guidelines and other documentation to support and guide compliance with information security policies
	Establish and maintain a program for information security awareness and training to promote a secure environment and an effective security culture
	Integrate information security requirements into organizational processes (for example, change control, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security baseline
	Integrate information security requirements into contracts and activities of third parties (for example, joint ventures, outsourced providers, business partners, customers) to maintain the organization's security baseline
	Establish, monitor and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program
	Knowledge of methods to align information security program requirements with those of other business functions
	Knowledge of methods to identify, acquire, manage and define requirements for internal and external resources

Knowledge Area	Understanding Demonstrated
	Knowledge of information security technologies, emerging trends, (for example, cloud computing, mobile computing) and underlying concepts
	Knowledge of methods to design information security controls
	Knowledge of information security architectures (for example, people, processes, technology) and methods to apply them
	Knowledge of methods to develop information security standards, procedures and guidelines
	Knowledge of methods to implement and communicate information security policies, standards, procedures and guidelines
	Knowledge of methods to establish and maintain effective information security awareness and training programs
	Knowledge of methods to integrate information security requirements into organizational processes
	Knowledge of methods to incorporate information security requirements into contracts and third-party management processes
	Knowledge of methods to design, implement and report operational information security metrics
	Knowledge of methods for testing the effectiveness and applicability of information security controls
Information Security Incident Management	Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate identification of and response to incidents
	Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents
	Develop and implement processes to ensure the timely identification of information security incidents
	Establish and maintain processes to investigate and document information security incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organizational requirements
	Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management
	Organize, train and equip teams to effectively respond to information security incidents in a timely manner
	Test and review the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities
	Establish and maintain communication plans and processes to manage communication with internal and external entities
	Conduct post-incident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions
	Establish and maintain integration among the incident response plan, disaster recovery plan and business continuity plan
	Knowledge of the components of an incident response plan
	Knowledge of incident management concepts and practices
	Knowledge of business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan
	Knowledge of incident classification methods
	Knowledge of damage containment methods
	Knowledge of notification and escalation processes
	Knowledge of the roles and responsibilities in identifying and managing information security incidents
	Knowledge of the types and sources of tools and equipment required to adequately equip incident response teams
	Knowledge of forensic requirements and capabilities for collecting, preserving

Knowledge Area	Understanding Demonstrated
	and presenting evidence (for example, admissibility, quality and completeness of evidence, chain of custody)
	Knowledge of internal and external incident reporting requirements and procedures
	Knowledge of post-incident review practices and investigative methods to identify root causes and determine corrective actions
	Knowledge of techniques to quantify damages, costs and other business impacts arising from information security incidents
	Knowledge of technologies and processes that detect, log and analyze information security events
	Knowledge of internal and external resources available to investigate information security incidents

**Table G.6.** Certified in Risk and Information Systems Control (CRISC)

Knowledge Area	Understanding Demonstrated
Risk Identification, Assessment and Evaluation	Collect information and review documentation to ensure that risk scenarios are identified and evaluated
	Identify legal, regulatory and contractual requirements and organizational policies and standards related to information systems to determine their potential impact on the business objectives
	Identify potential threats and vulnerabilities for business processes, associated data and supporting capabilities to assist in the evaluation of enterprise risk
	Create and maintain a risk register to ensure that all identified risk factors are accounted for
	Assemble risk scenarios to estimate the likelihood and impact of significant events to the organization
	Analyze risk scenarios to determine their impact on business objectives
	Develop a risk awareness program and conduct training to ensure that stakeholders understand risk and contribute to the risk management process and to promote a risk-aware culture
	Correlate identified risk scenarios to relevant business processes to assist in identifying risk ownership
	Validate risk appetite and tolerance with senior leadership and key stakeholders to ensure alignment
	Knowledge of standards, frameworks and leading practices related to risk identification, assessment and evaluation
	Knowledge of techniques for risk identification, classification, assessment and evaluation
	Knowledge of quantitative and qualitative risk evaluation methods
	Knowledge of business goals and objectives
	Knowledge of organizational structures
	Knowledge of risk scenarios related to business processes and initiatives
	Knowledge of business information criteria
	Knowledge of threats and vulnerabilities related to business processes and initiatives
	Knowledge of information systems architecture (e.g., platforms, networks, application, databases and operating systems)
	Knowledge of information security concepts
	Knowledge of threats and vulnerabilities related to third-party management
	Knowledge of threats and vulnerabilities related to data management
	Knowledge of threats and vulnerabilities related to the system development life cycle

Knowledge Area	Understanding Demonstrated
	Knowledge of threats and vulnerabilities related to project and program management
	Knowledge of threats and vulnerabilities related to business continuity and disaster recovery management
	Knowledge of threats and vulnerabilities related to management of IT operations
	Knowledge of the elements of a risk register
	Knowledge of risk scenario development tools and techniques
	Knowledge of risk awareness training tools and techniques
	Knowledge of principles of risk ownership
	Knowledge of current and forthcoming laws, regulations and standards
	Knowledge of threats and vulnerabilities associated with emerging technologies
Risk Response	Identify and evaluate risk response options and provide management with information to enable risk response decisions
	Review risk responses with the relevant stakeholders for validation of efficiency, effectiveness and economy
	Apply risk criteria to assist in the development of the risk profile for management approval
	Assist in the development of risk response action plans to address risk factors identified in the organizational risk profile
	Assist in the development of business cases supporting the investment plan to ensure risk responses are aligned with the identified business objectives
	Knowledge of standards, frameworks and leading practices related to risk response
	Knowledge of risk response options
	Knowledge of cost-benefit analysis and return on investment (ROI)
	Knowledge of risk appetite and tolerance
	Knowledge of organizational risk management policies
	Knowledge of parameters for risk response selection
	Knowledge of project management tools and techniques
	Knowledge of portfolio, investment and value management
	Knowledge of exception management
	Knowledge of residual risk
Risk Monitoring	Collect and validate data that measure key risk indicators (KRIs) to monitor and communicate their status to relevant stakeholders
	Monitor and communicate key risk indicators (KRIs) and management activities to assist relevant stakeholders in their decision-making process
	Facilitate independent risk assessments and risk management process reviews to ensure they are performed efficiently and effectively
	Identify and report on risk, including compliance, to initiate corrective action and meet business and regulatory requirements
	Knowledge of standards, frameworks and leading practices related to risk monitoring
	Knowledge of principles of risk ownership
	Knowledge of risk and compliance reporting requirements, tools and techniques
	Knowledge of key performance indicator (KPIs) and key risk indicators (KRIs)
	Knowledge of risk assessment methodologies
	Knowledge of data extraction, validation, aggregation and analysis tools and techniques
	Knowledge of various types of reviews of the organization's risk monitoring process (e.g. internal and external audits, peer reviews, regulatory reviews, quality reviews)



<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
Information Systems Control Design and Implementation	Interview process owners and review process design documentation to gain an understanding of the business process objectives
	Analyze and document business process objectives and design to identify required information systems controls
	Design information systems controls in consultation with process owners to ensure alignment with business needs and objectives
	Facilitate the identification of resources (e.g., people, infrastructure, information, architecture) required to implement and operate information systems controls at an optimal level
	Monitor the information systems control design and implementation process to ensure that it is implemented effectively and within time, budget and scope
	Provide progress reports on the implementation of information systems controls to inform stakeholders and to ensure that deviations are promptly addressed
	Test information systems controls to verify effectiveness and efficiency prior to implementation
	Implement information systems controls to mitigate risk
	Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of information systems control performance in meeting business objectives
	Assess and recommend tools to automate information systems control processes
	Provide documentation and training to ensure information systems controls are effectively performed
	Ensure all controls are assigned control owners to establish accountability
	Establish control criteria to enable control life- cycle management
	Knowledge of standards, frameworks and leading practices related to information systems control design and implementation
	Knowledge of business process review tools and techniques
	Knowledge of testing methodologies and practices related to information systems control design and implementation
	Knowledge of control practices related to business processes and initiatives
	Knowledge of the information systems architecture (e.g., platforms, networks, application, databases and operating systems)
	Knowledge of controls related to information security
	Knowledge of controls related to third-party management
	Knowledge of controls related to data management
	Knowledge of controls related to the system development life cycle
	Knowledge of controls related to project and program management
	Knowledge of controls related to business continuity and disaster recovery management
	Knowledge of controls related to management of IT operations
	Knowledge of software and hardware certification and accreditation practices
	Knowledge of the concept of control objectives
	Knowledge of governance, risk and compliance (GRC) tools
	Knowledge of tools and techniques to educate and train users
IS Control Monitoring and Maintenance	Plan, supervise and conduct testing to confirm continuous efficiency and effectiveness of information systems controls
	Collect information and review documentation to identify information systems control deficiencies
	Review information systems policies, standards and procedures to verify that they address the organization's internal and external requirements
	Assess and recommend tools and techniques to automate information systems control verification processes
	Evaluate the current state of information systems processes using a maturity

Knowledge Area	Understanding Demonstrated
	model to identify the gaps between current and targeted process maturity
	Determine the approach to correct information systems control deficiencies and maturity gaps to ensure that deficiencies are appropriately considered and remediated
	Maintain sufficient, adequate evidence to support conclusions on the existence and operating effectiveness of information systems controls
	Provide information systems control status reporting to relevant stakeholders to enable informed decision making
	Knowledge of standards, frameworks and leading practices related to information systems control monitoring and maintenance
	Knowledge of enterprise security architecture
	Knowledge of monitoring tools and techniques
	Knowledge of maturity models
	Knowledge of control objectives, activities and metrics related to IT operations and business processes and initiatives
	Knowledge of control objectives, activities and metrics related to incident and problem management
	Knowledge of security testing and assessment tools and techniques
	Knowledge of control objectives, activities and metrics related to architecture (platforms, networks, application, databases and operating systems)
	Knowledge of control objectives, activities and metrics related to information security
	Knowledge of control objectives, activities and metrics related to third-party management
	Knowledge of control objectives, activities and metrics related to data management
	Knowledge of control objectives, activities and metrics related to the system development life cycle
	Knowledge of control objectives, activities and metrics related to project and program management
	Knowledge of control objectives, activities and metrics related to software and hardware certification and accreditation practices
	Knowledge of control objectives, activities and metrics related to business continuity and disaster recovery management
	Knowledge of applicable laws and regulations

**Table G.7.** Certified Incident Handler (GCIH)

Knowledge Area	Understanding Demonstrated
Backdoors and Trojan Horses	Demonstrate a detailed understanding of how Backdoors are used to gain access to systems, and how to defend systems
Buffer Overflows	Demonstrate an understanding of what a buffer overflow is, how they are created, and how to defend against them. Additionally, candidates will demonstrate a high-level understanding of how attackers use common tools to create and maintain a backdoor on a compromised system.
Covering Tracks: Networks	Demonstrate an understanding of how attackers use tunneling and covert channels to cover their tracks on a network, and the strategies involved in defending against them
Covering Tracks: Systems	Demonstrate an understanding of how attackers hide files and directories on Windows and Linux hosts and how they attempt to cover their tracks
Denial-of-Service Attacks	Demonstrate a comprehensive understanding of the different kinds of Denial of Service attacks and how to defend against them

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
Exploiting Systems using Netcat	Demonstrate an understanding of how to properly use the Netcat utility and how to defend against it
Format String Attacks	Demonstrate a comprehensive understanding of how format string attacks work and how to defend against them
Incident Handling Overview and Preparation	Demonstrate an understanding of what Incident Handling is, why it is important, and an understanding of best practices to take in preparation for an Incident
Incident Handling Phase 2: Identification	Demonstrate an understanding of important strategies to gather events, analyze them, and determine if we have an incident
Incident Handling Phase 3: Containment	Demonstrate an understanding of high-level strategies to prevent an attacker from causing further damage to the victim after discovering the incident
Incident Handling: Recovering and Improving Capabilities	Demonstrate an understanding of the general approaches to get rid of the attacker's artifacts on compromised machines, the general strategy to safely restore operations, and the importance of the incident report and "lessons learned" meetings
IP Address Spoofing	Demonstrate an understanding of what IP Spoofing is, the three different types of spoofing, and strategies to defend against it
Network Sniffing	Know what network sniffing is, how to use common sniffing tools, and how to defend against sniffers
Password Attacks	Demonstrate a detailed understanding of the three methods of password cracking
Reconnaissance	Demonstrate an understanding of public and open-source reconnaissance techniques
Rootkits	Demonstrate an understanding of how user-mode and kernel-mode rootkits operate, what their capabilities are and how to defend against them
Scanning: Host Discovery	Demonstrate an understanding of the tools and techniques used for host discovery on wired and wireless networks
Scanning: Network and Application Vulnerability Scanning and Tools	Demonstrate an understanding of the fundamentals of network and application vulnerability scanners, common commercial and open-source tools, and how to defend against them
Scanning: Network Devices (Firewall rules determination, fragmentation, and IDS/IPS evasion)	Demonstrate an understanding of how to use Firewalk to determine firewall policies, the general principles of IP fragmentation attacks, why they are used, as well as the ability to identify them
Scanning: Service Discovery	Demonstrate an understanding of the tools and techniques used for network mapping, port scanning, and passive fingerprinting techniques and how to defend against them
Session Hijacking, Tools and Defenses	Demonstrate an understanding of the definition of session hijacking, the two methods commonly used and why it is effective. Additionally, the candidate will demonstrate an understanding of how to identify common hijacking tools and the strategies to prepare for, identify and contain hijacking attacks.
Types of Incidents	Demonstrate an understanding of multiple types of incidents, including espionage, unauthorized use, intellectual property, and insider threats and apply strategies to prevent or address these cases
Virtual Machine Attacks	Demonstrate an understanding of the virtual machine environment from an attackers perspective, including targets and detection, and how to defend against threats
Web Application Attacks	Demonstrate an understanding of the value of the Open Web Application Security Project (OWASP), as well as different Web App attacks such as account harvesting, SQL injection, Cross-Site Scripting and other Web Session attacks

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
Worms, Bots and Bot-Nets	Demonstrate a detailed understanding of what worms, bots and bot-nets are, and how to protect against them

**Table G.8.** Certified Intrusion Analyst (GCIA)

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
Advanced Snort Concepts	Demonstrate a fundamental understanding of advanced Snort concepts such as rule ordering and reduction of false negatives and positives
Analyst Toolkit	Demonstrate an understanding of the different tools that are available when analyzing intrusions as well as typical uses for them
Domain Name System (DNS)	Demonstrate a thorough understanding of how DNS works for both legitimate and malicious purposes
Examining Packet Crafting	Demonstrate familiarity with how packets are crafted using different tools
Examining Packet Header Fields	Demonstrate a thorough understanding of what constitutes normal and abnormal values in IP, TCP, UDP, and ICMP header fields
Fragmentation	Demonstrate an understanding of how fragmentation works through theory and packet capture examples, as well as the concepts behind fragmentation-based attacks
ICMP Theory	Demonstrate an understanding of the ICMP protocol, how ICMP can be used for mapping, and the concepts behind ICMP based attacks
IDS/IPS Management and Architecture Issues	Demonstrate a thorough understanding of the management and architecture issues with regard to deploying IDS/IPS systems
Indications & Warnings and Traffic Correlation	Demonstrate knowledge of fundamental Indications and Warnings Analysis as well as techniques used to correlate traffic
IPv6	Demonstrate an understanding of IPv6 headers, the key differences between IPv4 and IPv6, and methods for implementing IPv6 over IPv4 networks
Microsoft Protocols	Demonstrate an understanding of Microsoft's® SMB/CIFS, RPC, and Active Directory protocols
Network Traffic Analysis	Demonstrate the ability to analyze real traffic: malicious, normal and application traffic; and demonstrate the ability to discern malicious traffic from false positives
NIDS Evasion, Insertion, and Checksums	Demonstrate a fundamental understanding of the evasion and insertion techniques hackers utilize to confuse systems and how checksums function
Snort Fundamentals and Configuration	Demonstrate a fundamental understanding of the installation of Snort, its modes of operation, and how to configure it
Snort GUIs and Sensor Management	Demonstrate familiarity with GUI tools that are available to manage a Snort implementation
Snort Performance, Active Response and Tagging	Demonstrate a fundamental understanding of Snort performance options, active response techniques, and tagging
Snort Rules	Demonstrate familiarity with how to effectively configure Snort rules
Stimulus Response	Demonstrate a fundamental understanding of how hosts respond to both normal and abnormal traffic
Tcpdump Fundamentals	Demonstrate a thorough understanding of how to analyze packet headers using tcpdump
TCP/IP Fundamentals	Demonstrate familiarity with tcpdump/windump, and demonstrate a thorough understanding of TCP/IP
Wireshark® Fundamentals	Demonstrate the ability to analyze traffic with Wireshark
Writing Tcpdump Filters	Demonstrate familiarity with the techniques that are involved when writing tcpdump filters

**Table G.9. Penetration Tester (GPEN)**

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
Advanced Hash Manipulation	Demonstrate an understanding of advanced techniques for breaking and using password hashes
Command Shell vs. Terminal Access	Demonstrate an understanding of the difference between shell and terminal access and the advantages of each
Enumerating Users	Demonstrate an understanding of the common ways to enumerate users during a pen-test and why it is important to do so
Exploitation Fundamentals	Demonstrate an understanding of the fundamental concepts associated with the exploitation phase of a pen-test
Injection Attacks	Demonstrate an understanding of the basic concepts associated with injection attacks
Legal Issues	Demonstrate an understanding of the legal issues that surround pen-testing
Metasploit	Demonstrate an understanding of Metasploit and how it can be used during a pen-test
Moving Files with Exploits	Demonstrate an understanding of how to use exploits to move files between remote systems
Obtaining and Passing Password Representations	Demonstrate an understanding of the various ways to obtain password hashes from a target system during a pen-test
Overview of Passwords	Demonstrate an understanding of the various password types and formats
Pen-testing Foundations	Demonstrate an understanding of the fundamental concepts associated with pen-testing
Pen-testing Process	Demonstrate an understanding of the pen-testing process and the importance of reporting
Pen-Testing via the Command Line	Demonstrate an understanding of the Windows command line and other command shells that can be used during a pen-test
Profiling the Target	Demonstrate an understanding of how to conduct port, operating system and service version scans and their purpose during a pen-test
Reconnaissance	Demonstrate an understand of the basic concepts of reconnaissance and how to obtain basic information during this phase
Scanning for Targets	Demonstrate an understanding of the fundamental concepts associated with the scanning phase, and the value of network sweeping and tracing as part of a pen-test
Using a Proxy to Attack a Web Application	Demonstrate an understanding of how to use a web proxy during a pen-test to look for web-based weaknesses
Vulnerability Scanning	Demonstrate an understanding of the importance of vulnerability scanning and how to interpret the results
Wireless Crypto and Client Attacks	Demonstrate an understanding of the various types of wireless cryptographic and client attacks that can be used during a pen-test
Wireless Fundamentals	Demonstrate an understanding of the fundamental concepts associated with wireless networks as they relate to a pen-test

**Table G.10. Web Application Penetration Tester (GWAPT)**

<b>Knowledge Area</b>	<b>Understanding Demonstrated</b>
AJAX	Demonstrate an understanding of AJAX technology and its known weaknesses
Automated Web Application Vulnerability Scanners	Demonstrate familiarity with automated tools used to find web application vulnerabilities and their distinguishing features
Cross Site Scripting and Attack Frameworks	Demonstrate an understanding of the types of XSS attacks and XSS attack frameworks that can be utilized during a pen test
Flash	Demonstrate comprehension of Flash technology and its weaknesses
Programming Fundamentals	Demonstrate familiarity with modern web-based languages including Javascript with Ajax, Java Applets, PHP, and Python
Recon Using Public Information	Demonstrate comprehension of techniques used to conduct reconnaissance using publicly available information
Scanning and Mapping	Demonstrate an understanding of mapping and scanning web applications and servers, including port scanning, identifying services and configurations, spidering, application flow charting and session analysis
Session Tracking and SSL	Demonstrate comprehension of session tracking and SSL/TLS use in modern web communications as well as the attacks that can leverage flaws in session state
SQL Injection	Demonstrate an understanding of how to perform SQL injection attacks and how to identify SQL injection vulnerabilities in applications
Understanding the Web and HTTP	Demonstrate an understanding of the fundamentals web applications and their architecture and a thorough comprehension of the HTTP protocol
Web App Pen Test Methodology and Reporting	Demonstrate comprehension of the typical methods and components used during a web application penetration test
Web Services	Demonstrate familiarity with web service technologies and attack vectors

## **Appendix H**

### **Job Responsibilities and Responsibility Areas**





## Appendix H

### Job Responsibilities and Responsibility Areas

The table below shows how the job responsibilities developed in Phase 1 of this project were mapped to the responsibility areas developed and used in Phase 2. This mapping was conducted by the Subject Matter Expert (SME) panel leadership and National Board of Information Security Examiners staff.

**Table H.1.** Mapping of Phase I Job Responsibilities to Responsibility Areas

Responsibility Areas	Job Responsibilities from SGC Phase I
Analyze Security Incidents	Ensure a baseline of normal/expected activity is available or can be quickly assembled to support analysis
	Ensure all internal experts and responsible parties are consulted and engaged to analyze security incidents
	Ensure that a methodology has been established for evaluating alert types and that those thresholds are programmed into the security monitoring solution by impact level
Assess and Manage Risk	Ensure models exists to assess security risk
	Ensure vendors are contractually notifying you of exposures and security issues of interest—a nondisclosure agreement will usually be required for full transparency
	Ensure you understand application, OS and infrastructure to identify which tools best mitigate business risks
Communicate Results	Ensure appropriate stakeholders and security management receive security metrics
	Ensure communication plans are updated
	Ensure system owners are aware of activities prior to performing assessments
	Ensure that you communicate with vendors who make your smart grid components and request that they provide you with information related to vulnerabilities that they identify
Develop and Manage Personnel	Ensure that personnel responsible for investigating security events understand what constitutes an actual event
	Ensure only authorized staff can access security tools and data
	Ensure security staff understands company policies and technical standards
	Ensure all stakeholders are identified and contact information is available to determine reporting requirements and make reports
	Ensure security operations staff are proficient with security tools and understand their capabilities and constraints
	Ensure adequate and representative environments exists to train staff and evaluate threats and vulnerabilities and their mitigations
	Ensure all security operations staff and stakeholders maintain an understanding of applicable vulnerabilities and threats
	Ensure all training scenarios are current and match your organization's attack technique table
	Ensure Incident Response Specialist has been trained and current in latest threats analysis
	Ensure ongoing training with refresher courses on current and future toolset or techniques
	Ensure operational security staff maintains a current understanding of Attack and Defense TTPs
	Ensure that all employees regardless of rank/role are familiar with the most basic usages of office-wide security software, and know where to turn if an issue arises

<b>Responsibility Areas</b>	<b>Job Responsibilities from SGC Phase I</b>
Identify and Mitigate Vulnerabilities	Ensure the organization conducts “lessons learned” with every material incident
	Ensure the organization maintains an attack technique table with detailed TTPs
	Ensure all vulnerabilities are tracked and mitigated in a timely manner
	Ensure all vulnerability and assessment findings are prioritized according to risk
	Ensure hardening of operating system, services, and applications on custom or third-party solutions
	Ensure maintenance of security profiles for smart grid components
	Ensure reasonable effort and capability to test deployed assets and smart grid devices
	Ensure that smart grid security components are put through an annual vulnerability assessment so that weaknesses can be identified
	Ensure that you have set up your vulnerability scanning solution to routinely scan and identify assets for vulnerabilities
	Ensure vulnerability assessment solution is configured to provide the desired results
	Ensure vulnerability scanner is tested adequately to operate in the target environment
Implement Security Monitoring	Ensure all appropriate parties are consulted and support security tool implementation
	Ensure all functional requirements meet current needs and identify tools that fall short
	Ensure independent review of installation of security monitoring solutions to assess effectiveness and coverage
	Ensure monitoring can be automated or scripted
	Ensure monitoring of security state of your organization’s systems and assets
	Ensure monitoring solution is configured correctly to obtain vendor software and signature updates
	Ensure that all assets that require monitoring are logging to the security monitoring solution and that you are able to identify each asset that is supposed to be logging
	Ensure that you are monitoring security threat websites so that you are getting vulnerability information about assets that are in place in your network and whether or not vendors have released patches or firmware upgrades to correct those security issues
	Ensure the security monitoring solution satisfies all organizational monitoring requirements
Log Security Incidents	Ensure logging and security information is stored for analysis for an appropriate period of time
	Ensure rigor and completeness of security log and information analysis
	Ensure sufficient artifacts are available to make determination
	Ensure that security event types have been defined by classification; for example, unauthorized access attempts to a firewall may not be considered an incident, unless they meets a certain threshold (five attempts to the firewall may not be an incident, but 5000 attempts from the same IP address may be an indication of a DoS attack)
	Ensure all data and evidence associated with intrusions are stored in an appropriate manner
	Ensure all security incident reporting requirements are satisfied properly
	Ensure incident data is collected, analyzed, maintained, and reviewed
	Ensure all security events have been identified
	Ensure false positives are tracked, provide advice for future filtering and close ticket
	Ensure log sources are time-synced to a local Network Time Protocol (NTP)

<b>Responsibility Areas</b>	<b>Job Responsibilities from SGC Phase I</b>
	server
	Ensure that you are receiving notifications from vendors in the case where they have been breached and maintain access to your networks
	Ensure all incidents are classified into categories and provide data back to stakeholders, management, and the risk assessment process
	Ensure all security information regarding exposure, threats, and protective measures is provided to develop appropriate risk picture
	Ensure maintenance of an accurate picture of utility systems deployed, architectures, communication protocols employed and business functions and processes
Manage Process and Procedures	Ensure incident response and recovery procedures are tested regularly
	Ensure the incident response procedure/plan is executed and followed
Manage Projects and Budgets	Ensure adequate budget has been apportioned for monitoring solution
	Ensure all solutions being installed have been authorized
	Ensure all security projects are managed for budget, progress, and risk
	Ensure budget is built into role to adequately address skill set improvement, training and certifications
	Ensure company policies and procedures are followed for configuration management
Manage Security Operations	Ensure all operations and response activities are prioritized by Business Impact Assessment results
	Ensure security tools are patched and updated properly
	Ensure Security Information and Event Management (SIEM) system is operating to expected functional and/or performance requirements
	Ensure company policies and procedures are followed for downloading and installing third-party software
Respond to Intrusions	Ensure all intrusions are contained properly
	Ensure all intrusions are eradicated or cleaned to the greatest extent possible
	Ensure all open intrusions are managed in a timely manner
	Ensure intrusions are closed by verifying incident response actions and testing targeted environment for additional attacker activity



## **Appendix I**

### **Assignment of Certifications to Job Responsibilities**



# Appendix I

## Assignment of Certifications to Job Responsibilities

This appendix provides the summarized results from the subject matter expert panel votes mapping the credentialing exams to the job responsibilities identified in Phase I of this project.

### I.1 Summary of Results for Mapping of Responsibilities to Credentialing Programs

Listed below are the responsibilities assigned by the panel to the four job roles analyzed. The total number of responsibilities for each role is listed in parentheses after the job role title. Under each responsibility is listed the certifications that include learning objectives (number in parentheses) that were determined by the panel to be related to that responsibility. However, since each certification differs in the degree of detail provided for its learning objectives, these numbers should not be considered an indication of the breadth of coverage for a particular responsibility. Therefore, the analysis below will focus on simply the number of responsibility areas each certification covers with at least one learning objective. Responsibilities that are listed without a certification assigned indicate areas needing development of credentialing exam items.

#### I.1.1 Cyber Secure Power Engineer Responsibilities

Panel members associated the following two certifications' learning objectives with one or more job responsibilities associated with the Cyber Secure Power Engineer:

- Certified Information Security Manager (CISM) – ISACA
- Certified Information Systems Security Professional (CISSP) – ISC<sup>2</sup>

Panel members associated one or more certification learning objectives with three of the nine job responsibilities associated with the Cyber Secure Power Engineer. Below are the nine job responsibilities for the Cyber Secure Power Engineer along with a listing of any certifications that have one or more learning objectives that mapped to that job responsibility (note: the responsibilities are only the security subset of an engineer responsible for managing energy control systems) The number in parentheses next to the certification acronym is the number of that certification's learning objectives that panel members associated with that responsibility:

- Ensure a baseline of normal/expected activity is available or can be quickly assembled to support analysis.
- Ensure all appropriate parties are consulted and support security tool implementation.
  - CISM (2)
  - CISSP (3)

- Ensure all functional requirements meet current needs and identify tools that fall short.
  - CISSP (5)
- Ensure hardening of operating system, services, and applications on custom or third-party solutions.
- Ensure maintenance of an accurate picture of utility systems deployed, architectures, communication protocols employed and business functions and processes.
- Ensure reasonable effort and capability to test deployed assets and smart grid devices.
- Ensure that all assets that require monitoring are logging to the security monitoring solution and that you are able to identify each asset that is supposed to be logging.
- Ensure that you communicate with vendors who make your smart grid components and request that they provide you with information related to vulnerabilities that they identify.
- Ensure you understand application, operating systems and infrastructure to identify which tools best mitigate business risks.
  - CISSP (6)

### **I.1.2 Incident Response Specialist Responsibilities**

Panel members associated the following three certifications' learning objectives with one or more job responsibilities associated with the Incident Response Specialist:

- Certified Information Security Manager (CISM) – ISACA
- Certified Information Systems Security Professional (CISSP) – ISC<sup>2</sup>
- Certified Incident Handler (GCIH) – GIAC

Panel members associated one or more certification learning objectives with 10 of the 10 job responsibilities associated with the Incident Response Specialist. Below are the 10 job responsibilities for the Incident Response Specialist along with a listing of any certifications that have one or more learning objectives that mapped to that job responsibility. The number in parentheses next to the certification acronym is the number of that certification's learning objectives that panel members associated with that responsibility:

- Ensure all data and evidence associated with intrusions is stored in an appropriate manner.
  - CISM (3)
- Ensure all incidents are classified into categories and provide data back to stakeholders, management, and risk assessment process.
  - CISM (10)
  - GCIH (3)
- Ensure all intrusions are contained properly.
  - GCIH (4)



- Ensure all intrusions are eradicated or cleaned to the greatest extent possible.
  - GCIH (3)
- Ensure all open intrusions are managed in a timely manner.
  - CISSP (1)
  - GCIH (4)
- Ensure all security events have been identified.
  - CISM (3)
  - GCIH (1)
- Ensure all security incident reporting requirements are satisfied properly.
  - CISM (7)
  - GCIH (3)
- Ensure incident data is collected, analyzed, maintained, and reviewed.
  - GCIH (5)
- Ensure Incident response and recovery procedures are tested regularly.
  - CISSP (2)
  - GCIH (4)
- Ensure the incident response procedure/plan is executed and followed.
  - CISSP (1)
  - GCIH (5)

### **I.1.3 Intrusion Analyst Responsibilities**

Panel members associated the following five certifications' learning objectives with one or more job responsibilities associated with the Intrusion Analyst:

- Certified Information Security Manager (CISM) – ISACA
- Certified Information Systems Security Professional (CISSP) – ISC<sup>2</sup>
- Certified Incident Handler (GCIH) – GIAC
- Certified Ethical Hacker (CEH) – EC-Council
- Certified Intrusion Analyst (GCIA) – GIAC

Panel members associated one or more certification learning objectives with 8 of the 10 job responsibilities associated with the Intrusion Analyst. Below are the 10 job responsibilities for the Intrusion Analyst along with a listing of any certifications that have one or more learning objectives that mapped to that job responsibility. The number in parentheses next to the certification acronym is the number of that certification's learning objectives that panel members associated with that responsibility:

- Ensure a baseline of normal/expected activity is available or can be quickly assembled to support analysis.
- Ensure all data and evidence associated with intrusions is stored in an appropriate manner.
  - CISM (3)
- Ensure all incidents are classified into categories and provide data back to stakeholders, management, and the risk assessment process.
  - CISM (10)
  - GCIH (3)
- Ensure all intrusions are contained properly.
  - GCIH (4)
- Ensure all intrusions are eradicated or cleaned to the greatest extent possible.
  - GCIH (3)
- Ensure all open intrusions are managed in a timely manner.
  - CISSP (1)
  - GCIH (4)
- Ensure all security events have been identified.
  - CISM (3)
  - GCIH (1)
- Ensure incident data is collected, analyzed, maintained, and reviewed.
  - GCIH (5)
- Ensure intrusions are closed by verifying incident response actions and testing the targeted environment for additional attacker activity.
  - CEH (5)
  - CISSP (2)
  - GCIA (6)
  - GCIH (5)
- Ensure that security event types have been defined by classification; for example, unauthorized access attempts to a firewall may not be considered an incident, unless it meets a certain threshold (five attempts to the firewall may not be an incident, but 5000 attempts from the same IP address may be an indication of a DoS attack).

#### **I.1.4 Security Operations Specialist Responsibilities**

Panel members associated the following three certifications' learning objectives with one or more job responsibilities associated with the Security Operations Specialist:

- Certified Information Security Manager (CISM) – ISACA
- Certified Information Systems Security Professional (CISSP) – ISC<sup>2</sup>
- Certified Incident Handler (GCIH) – GIAC

Panel members associated one or more certification learning objectives with 11 of the 16 job responsibilities associated with the Security Operations Specialist. Below are the 16 job responsibilities for the Security Operations Specialist along with a listing of any certifications that have one or more learning objectives that mapped to that job responsibility. The number in parentheses next to the certification acronym is the number of that certification's learning objectives that panel members associated with that responsibility:

- Ensure a baseline of normal/expected activity is available or can be quickly assembled to support analysis.
- Ensure all appropriate parties are consulted and support security tool implementation.
  - CISM (2)
  - CISSP (3)
- Ensure all data and evidence associated with intrusions are stored in an appropriate manner.
  - CISM (3)
- Ensure all incidents are classified into categories and provide data back to stakeholders, management, and the risk assessment process.
  - CISM (10)
  - GCIH (3)
- Ensure all security events have been identified.
  - CISM (3)
  - GCIH (1)
- Ensure all security incident reporting requirements are satisfied properly.
  - CISM (7)
  - GCIH (3)
- Ensure all security information regarding exposure, threats, and protective measures is provided to develop appropriate risk picture.
  - CISM (11)
  - CISSP (1)
- Ensure all security operations staff and stakeholders maintain an understanding of applicable vulnerabilities and threats.
- Ensure all solutions being installed have been authorized.
  - CISSP (2)

- Ensure logging and security information is stored for analysis for an appropriate period of time.
  - CISM (1)
  - CISSP (1)
- Ensure maintenance of security profiles for smart grid components.
  - CISSP (1)
- Ensure monitoring of the security state of your organization's systems and assets.
  - CISM (5)
  - CISSP (1)
- Ensure only authorized staff can access security tools and data.
- Ensure operational security staff maintains a current understanding of Attack and Defense TTPs.
- Ensure security tools are patched and updated properly.
  - CISSP (2)
- Ensure Security Information and Event Management system is operating to expected functional and/or performance requirements.

At first glance, it appears that credentialing programs have reasonable coverage of the responsibilities for three smart grid cybersecurity job roles (Incident Response, Intrusion Analysis, and Security Operations). However, none of the credentialing programs is comprehensive, they all demonstrate inconsistent breadth, and there are insufficient items in these exams to cover the over 500 tasks identified during the prior phase as needed to fulfill the responsibilities of these jobs. In addition to expanding coverage to include all responsibilities for a job role, future research on credentialing should explore how to develop a richer collection of exam items necessary to cover the tasks determined as fundamental to and differentiating of job performance as outlined in the Phase I report.

## **Appendix J**

### **Mapping of Competency Model Frameworks and Course Topics to Responsibility Areas**



## Appendix J

### Mapping of Competency Model Frameworks and Course Topics to Responsibility Areas

This appendix provides the summarized and detailed results from the subject matter expert panel votes to map the two competency model frameworks (National Initiative for Cybersecurity Education [NICE] and Electric Subsector Cybersecurity Capability Maturity Model [ES-C2M2]) and the course topics to job responsibilities identified in Phase I of this project. The first section (J.1.) in this appendix briefly summarizes the findings and the subsequent sections (J.2, J.3, J.4) are the detailed results for each of these mapping exercises.

#### J.1 Summary of Results for Mapping of Responsibilities to the NICE Framework, ES-C2M2 Framework, and the Course Topics

Responsibility areas were mapped to the NICE tasks, ES-C2M2 performance objectives, and training and education course topics. The eleven responsibility areas are listed below followed by each of the workforce program items that received votes equal to or above the cutoff score appropriate for that program. The task number that NICE assigned to each task is shown at the end of each task item.

##### J.1.1 Analyze Security Incidents

Panel members associated 14 NICE tasks, two ES-C2M2 tasks, and two course topics with the Analyze Security Incidents responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (14)
  - Assist in the construction of signatures that can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise; 427
  - Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources; 433
  - Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise; 438
  - Coordinate with enterprise-wide Computer Network Defense staff to validate network alerts; 472
  - Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation; 478
  - Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation; 743

- Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of suspected Computer Network Defense incidents and articulate the event’s history, status, and potential impact for further action; 723
- Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security; 738
- Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack; 750
- Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems; 755
- Perform real-time Computer Network Defense Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs); 762
- Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts; 823
- Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.; 846
- Track and document Computer Network Defense incidents from initial detection through final resolution; 861
- C2M2 Tasks (2)
  - Detect Cybersecurity Events
  - Identify and Respond to Threats
- Course Topics (2)
  - Cyber asset vulnerabilities, access, and attack vector identification
  - Cyber threats, attacks, and mitigations to control systems

## **J.1.2 Assess and Manage Risk**

Panel members associated nine NICE tasks, four ES-C2M2 tasks, and nine course topics with the Assess and Manage Risk responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (9)
  - Analyze site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives; 411
  - Coordinate with intelligence analysts to correlate threat assessment data; 474
  - Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation; 478



- Identify potential conflicts with implementation of any Computer Network Defense tools within the Computer Network Defense service provider area of responsibility (e.g., tool/signature testing and optimization); 643
- Maintain deployable Computer Network Defense audit toolkit (e.g., specialized Computer Network Defense software/hardware) to support Computer Network Defense audit missions; 685
- Maintain knowledge of applicable Computer Network Defense policies, regulations, and compliance documents specifically related to Computer Network Defense auditing; 692
- Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise; 716
- Perform Computer Network Defense risk assessments within the enterprise; 744
- Perform Computer Network Defense vulnerability assessments within the enterprise; 746
- C2M2 Tasks (4)
  - Establish Cybersecurity Risk Management Strategy
  - Manage Cybersecurity Risk
  - Manage Dependency Risk
  - Manage RISK Activities
- Course Topics (9)
  - Architectural security and strategies
  - Control system network security
  - Control system security for field devices and communications
  - Control system security standards and compliance
  - Control system security testing (active and passive techniques)
  - Cyber threats, attacks, and mitigations to control systems
  - Defensive techniques and measures
  - Risk management
  - Wireless technology

### **J.1.3 Communicate Results**

Panel members associated 11 NICE tasks, three ES-C2M2 tasks, and zero course topics with the Communicate Results responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (11)

- Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents; 470
- Coordinate with intelligence analysts to correlate threat assessment data; 474
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation; 478
- Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of suspected Computer Network Defense incidents and articulate the event’s history, status, and potential impact for further action; 723
- Perform Computer Network Defense trend analysis and reporting; 745
- Perform Computer Network Defense vulnerability assessments within the enterprise; 746
- Perform real-time Computer Network Defense Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs); 762
- Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions; 784
- Provide daily summary reports of network events and activity relevant to Computer Network Defense practices; 800
- Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.; 846
- Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies; 882
- C2M2 Tasks (3)
  - Escalate Cybersecurity Events
  - Increase Cybersecurity Awareness
  - Share Cybersecurity Information
- Course Topics (0)

#### **J.1.4 Develop and Manage Personnel**

Panel members associated zero NICE tasks, four ES-C2M2 tasks, and one course topic with the Develop and Manage Personnel responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (0)
- C2M2 Tasks (4)
  - Control the Workforce Life cycle
  - Develop Cybersecurity Workforce

- Increase Cybersecurity Awareness
- Manage WORKFORCE Activities
- Course Topics (1)
  - Manage WORKFORCE Activities

### **J.1.5 Identify and Mitigate Vulnerabilities**

Panel members associated 11 NICE tasks, two ES-C2M2 tasks, and 11 course topics with the Identify and Mitigate Vulnerabilities responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (11)
  - Assist in the construction of signatures which can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise; 427
  - Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources; 433
  - Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise; 438
  - Conduct authorized penetration testing of enterprise network assets; 448
  - Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents; 470
  - Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation; 478
  - Maintain deployable Computer Network Defense audit toolkit (e.g., specialized Computer Network Defense software/hardware) to support Computer Network Defense audit missions; 685
  - Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation; 743
  - Perform Computer Network Defense risk assessments within the enterprise; 744
  - Perform Computer Network Defense vulnerability assessments within the enterprise; 746
  - Perform real-time Computer Network Defense Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs); 762
- C2M2 Tasks (2)
  - Identify and Respond to Threats
  - Reduce Cybersecurity Vulnerabilities

- Course Topics (11)
  - Architectural security and strategies
  - Control system network security
  - Control system security for field devices and communications
  - Control system security testing (active and passive techniques)
  - Control systems security for applications
  - Control systems security for hosts
  - Cyber asset vulnerabilities, access, and attack vector identification
  - Cyber threats, attacks, and mitigations to control systems
  - Defensive techniques and measures
  - Network security
  - Wireless technology

### **J.1.6 Implement Security Monitoring**

Panel members associated two NICE tasks, one ES-C2M2 task, and six course topics with the Implement Security Monitoring responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (2)
  - Administer Computer Network Defense test bed and test and evaluate new Computer Network Defense applications, rules/signatures, access controls, and configurations of Computer Network Defense service provider managed platforms; 393
  - Purchase or build, install, configure, and test specialized hardware to be deployed at remote sites; 822
- C2M2 Tasks (1)
  - Detect Cybersecurity Events
- Course Topics (6)
  - Access control, monitoring, and authentication
  - Control system network security
  - Control system security for field devices and communications
  - Network security
  - Security monitoring
  - Wireless technology

### **J.1.7 Log Security Incidents**

Panel members associated one NICE task, two ES-C2M2 tasks, and three course topics with the Log Security Incidents responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (1)
  - Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources; 433
- C2M2 Tasks (2)
  - Detect Cybersecurity Events
  - Perform Logging
- Course Topics (3)
  - Control system security for field devices and communications
  - Cyber threats, attacks, and mitigations to control systems
  - Security monitoring

### **J.1.8 Manage Process and Procedures**

Panel members associated three NICE tasks, eight ES-C2M2 tasks, and two course topics with the Manage Process and Procedures responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (3)
  - Analyze site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives; 411
  - Implement C&A requirements for specialized Computer Network Defense systems within the enterprise, and document and maintain records for them; 654
  - Maintain knowledge of applicable Computer Network Defense policies, regulations, and compliance documents specifically related to Computer Network Defense auditing; 692
- C2M2 Tasks (8)
  - Establish and Maintain a Common Operating Picture
  - Establish and Maintain Cybersecurity Architecture
  - Establish Cybersecurity Risk Management Strategy
  - Manage ASSET Activities
  - Manage Changes to Assets
  - Manage CYBER Activities
  - Manage DEPENDENCIES Activities

- Plan for Continuity
- Course Topics (2)
  - Control system security policy
  - Control system security standards and compliance

### **J.1.9 Manage Projects and Budgets**

Panel members associated one NICE task, one ES-C2M2 task, and zero course topics with the Manage Projects and Budgets responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (1)
  - Purchase or build, install, configure, and test specialized hardware to be deployed at remote sites; 822
- C2M2 Tasks (1)
  - Sponsor Cybersecurity Program
- Course Topics (0)

### **J.1.10 Manage Security Operations**

Panel members associated three NICE tasks, eight ES-C2M2 tasks, and five course topics with the Manage Security Operations responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (3)
  - Administer Computer Network Defense test bed and test and evaluate new Computer Network Defense applications, rules/signatures, access controls, and configurations of Computer Network Defense service provider managed platforms; 393
  - Perform command and control functions in response to incidents; 741
  - Perform system administration on specialized Computer Network Defense applications and systems (e.g., anti-virus, audit/remediation, or VPN devices) to include installation, configuration, maintenance, and backup/restore; 769
- C2M2 Tasks (8)
  - Assign Cybersecurity Responsibilities
  - Escalate Cybersecurity Events
  - Establish and Maintain a Common Operating Picture
  - Establish Cybersecurity Program Strategy
  - Manage CYBER Activities
  - Manage RESPONSE Activities

- Manage SITUATION Activities
- Plan for Continuity
- Course Topics (5)
  - Architectural security and strategies
  - Control system security for field devices and communications
  - Control system security policy
  - Control system security standards and compliance
  - Network security

### **J.1.11 Respond to Intrusions**

Panel members associated 10 NICE tasks, three ES-C2M2 tasks, and one course topic with the Respond to Intrusions responsibility area. Below are the NICE tasks, ES-C2M2 tasks, and course topics associated with this responsibility area:

- NICE Tasks (10)
  - Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise; 438
  - Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents; 470
  - Perform command and control functions in response to incidents; 741
  - Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation; 743
  - Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of suspected Computer Network Defense incidents and articulate the event's history, status, and potential impact for further action; 723
  - Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems; 755
  - Perform real-time Computer Network Defense Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs); 762
  - Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts; 823
  - Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.; 846

- Track and document Computer Network Defense incidents from initial detection through final resolution; 861
- C2M2 Tasks (3)
  - Identify and Respond to Threats
  - Manage RESPONSE Activities
  - Respond to Escalated Cybersecurity Events
- Course Topics (1)
  - Incident response



## J.2 Detailed Results for Assignment of NICE Tasks to Responsibility Areas

NICE Tasks	Analyze security incidents	Assess and manage risk	Communicate results	Develop and manage personnel	Identify and mitigate vulnerabilities	Implement security monitoring	Log security incidents	Manage process and procedures	Manage projects and budgets
Administer Computer Network Defense test bed and test and evaluate new Computer Network Defense applications, rules/signatures, access controls, and configurations of Computer Network Defense service provider managed platforms; 393	5	9	7	3	8	10	2	8	4
Analyze site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives; 411	5	12	7		2	3	1	13	2
Assist in the construction of signatures which can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise; 427	12	7	4		10	7	5	2	
Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources; 433	13	7	7		11	7	11	1	
Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise; 438	16	4	7		10	4	8	3	
Conduct authorized penetration testing of enterprise network assets; 448	5	9	8	1	14	4	3	2	3
Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents; 470	9	6	12	7	10	4	6	6	2
Coordinate with Computer Network Defense Analysts to manage and administer the updating of rules and signatures (e.g., IDS/IPS, anti-virus, and content blacklists) for specialized Computer Network Defense applications; 471	5	6	7	2	8	7	4	8	1
Coordinate with enterprise-wide Computer Network Defense staff to validate network alerts; 472	11	4	9	3	6	4	5	6	2
Coordinate with intelligence analysts to correlate threat assessment data; 474	8	10	12	2	7	2	3	4	

NICE Tasks	Analyze security incidents	Assess and manage risk	Communicate results	Develop and manage personnel	Identify and mitigate vulnerabilities	Implement security monitoring	Log security incidents	Manage process and procedures	Manage projects and budgets
Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation; 478	13	10	10	1	12	4	5	1	
Create, edit, and manage changes to network access control lists on specialized Computer Network Defense systems (e.g., firewalls and intrusion prevention systems); 481	4	8	5	1	7	9	5	5	1
Identify potential conflicts with implementation of any Computer Network Defense tools within the Computer Network Defense service provider area of responsibility (e.g., tool/signature testing and optimization); 643	3	10	5		6	9	4	6	3
Implement C&A requirements for specialized Computer Network Defense systems within the enterprise, and document and maintain records for them; 654	2	8	9	2	4	4	4	12	4
Maintain deployable Computer Network Defense audit toolkit (e.g., specialized Computer Network Defense software/hardware) to support Computer Network Defense audit missions; 685	6	10	5	2	10	5	7	7	2
Maintain deployable Computer Network Defense toolkit (e.g., specialized Computer Network Defense software/hardware) to support incident response team mission; 686	6	2	2	3	6	5	1	6	2
Maintain knowledge of applicable Computer Network Defense policies, regulations, and compliance documents specifically related to Computer Network Defense auditing; 692	5	11	6	6	5	2	1	13	4
Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise; 716	8	10	8	4	9	3	4	2	
Perform command and- control functions in response to incidents; 741	8	1	9	5	7	2	5	7	2
Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation; 743	14	9	9	2	13	4	6	4	1

NICE Tasks	Analyze security incidents	Assess and manage risk	Communicate results	Develop and manage personnel	Identify and mitigate vulnerabilities	Implement security monitoring	Log security incidents	Manage process and procedures	Manage projects and budgets
Perform Computer Network Defense risk assessments within the enterprise; 744	6	15	6		11	1	3	6	2
Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of suspected Computer Network Defense incidents and articulate the event's history, status, and potential impact for further action; 723	10	4	13	1	4	2	7	4	
Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security; 738	12	7	8		9	8	13	2	
Perform Computer Network Defense trend analysis and reporting; 745	9	6	11		6	7	6	2	1
Perform Computer Network Defense vulnerability assessments within the enterprise; 746	6	12	10	1	14	2	3	3	1
Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack; 750	14	7	7	1	7	9	11	3	1
Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems; 755	14	5	6		9	4	8	4	
Perform real-time Computer Network Defense Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs); 762	13	8	10	1	12	9	13	4	1
Perform system administration on specialized Computer Network Defense applications and systems (e.g., anti-virus, Audit/Remediation, or VPN devices) to include installation, configuration, maintenance, and backup/restore; 769	4	5	3	1	7	7	4	8	2
Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions; 784	7	8	11		6			6	
Provide daily summary reports of network events and activity relevant to Computer Network Defense practices; 800	9	2	14		4	4	9	5	

<b>NICE Tasks</b>	Analyze security incidents	Assess and manage risk	Communicate results	Develop and manage personnel	Identify and mitigate vulnerabilities	Implement security monitoring	Log security incidents	Manage process and procedures	Manage projects and budgets
Purchase or build, install, configure, and test specialized hardware to be deployed at remote sites; 822	2	5	3	1	3	13	4	9	10
Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts; 823	12	5	5	1	7	7	10	4	
Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.; 846	12	4	14	3	6	1	6	2	
Track and document Computer Network Defense incidents from initial detection through final resolution; 861	14	5	9	2	8	3	11	3	
Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies; 882	8	6	12	1	4		2	6	1

\*Blocks shaded red indicate a NICE task that, based on the panelists' votes, map to the associated responsibility area.

### J.3 Detailed Results for Assignment of ES-C2M2 Performance Objectives to Responsibility Areas

ES-C2M2 Objective	Analyze security incidents	Assess and manage risk	Communicate results	Develop and manage personnel	Identify and mitigate vulnerabilities	Implement security monitoring	Log security incidents	Manage process and procedures	Manage projects and budgets	Manage security operations	Respond to intrusions
Assign cybersecurity responsibilities		1		9	1			9	6	11	
Control access	1	3		2	3	3	2	6	2	9	1
Control the workforce lifecycle		2	2	10	1			8	6	9	
Detect cybersecurity events	11	5	3		7	10	10	1		4	4
Develop cybersecurity workforce			2	13				5	5	6	
Escalate cybersecurity events	6	6	10	1	2	1	4	3	1	11	8
Establish and maintain a common operating picture	1		5	3	1	1	2	13	3	12	
Establish and maintain cybersecurity architecture	2	6	2	3	6	3	2	10	5	9	1
Establish and maintain identities		2		2	1	1		7	2	7	
Establish cybersecurity program strategy	2	4	6	3	2			8	8	11	
Establish cybersecurity risk management strategy	3	10	5	1	4	1		10	5	8	
Identify and respond to threats	11	9	5	1	12	7	7	2		6	12
Identify dependencies	2	6	2	3	6			6	2	5	
Increase cybersecurity awareness	1	1	10	10	2	1	1	7	1	5	1
Manage ACCESS Activities	2	4	2	1	1	3	3	8	5	7	1
Manage ASSET Activities	2	1	2	2	1			12	6	9	
Manage asset configuration		2		4	3	1	1	8	2	6	

ES-C2M2 Objective	Analyze security incidents	Assess and manage risk	Communicate results	Develop and manage personnel	Identify and mitigate vulnerabilities	Implement security monitoring	Log security incidents	Manage process and procedures	Manage projects and budgets	Manage security operations	Respond to intrusions
Manage asset inventory	1	3	1			2	1	7	6	6	
Manage changes to assets	1	1	4	2	2	1		11	5	7	
Manage CYBER Activities	1	2	1	6	2	1	1	10	7	13	1
Manage cybersecurity risk	1	12	5	1	6			7	5	9	
Manage DEPENDENCIES Activities		4	2	4	1			11	3	9	
Manage dependency risk	1	11	2		3			9	2	7	
Manage RESPONSE activities	6	2	3	2	2	2	4	8	4	10	11
Manage RISK activities	3	14	3	2	4	1	1	6	5	7	1
Manage SHARING activities		1	8	2				8	3	8	
Manage SITUATION activities	4	3	5	4	5	2	2	8	3	12	3
Manage THREAT activities	7	6	4	3	7	2	2	5	2	9	5
Manage WORKFORCE activities		2	2	13				9	8	9	
Monitor the function	2	4	2	1	1	6	5	6		6	2
Perform logging	3		5	1		6	14	3		3	
Perform secure software development	2	4	1	4	5	2		7	7	7	1
Plan for continuity	1	6	4	6	3			12	6	10	1
Reduce cybersecurity vulnerabilities	6	7	2	3	13	6	3	4	3	7	1
Respond to escalated cybersecurity events	9	7	7		7	1	2	4		9	11
Share cybersecurity information	3	5	13	1	2	2	3	2		4	2
Sponsor cybersecurity program	1	2	4	5				9	10	9	

\*Blocks shaded red indicate an ES-C2M2 objective that, based on the panelists' votes, map to the associated responsibility area.

## J.4 Detailed Results for Assignment of Education and Training Courses to Responsibility Areas

Course Topic	Analyze security incidents	Assess and manage risk	Communicate results	Develop and manage personnel	Identify and mitigate vulnerabilities	Implement security monitoring	Log security incidents	Manage process and procedures	Manage projects and budgets	Manage security operations	Respond to intrusions
Access control, monitoring, and authentication	3	6	1	4	6	11	6	8		6	3
Architectural security and strategies	5	14	6	2	13	7	3	7	3	9	1
Background of cybersecurity in control systems	4	8	2	7	7	3	1	1		6	1
Control system network security	6	10	6	3	11	9	8	4		6	4
Control system security for field devices and communications	8	13	6	4	13	11	11	8	5	9	8
Control system security policy	2	7	6	2	4	3	3	9	1	9	1
Control system security standards and compliance	5	10	7	2	8	7	5	11	3	11	2
Control system security testing (active and passive techniques)	5	10	8		12	6	4	3	1	7	1
Control systems security for applications	3	7	2	2	11	6	7	4	2	7	3
Control systems security for hosts	5	8	3	1	11	7	6	5	2	8	5
Cyber asset vulnerabilities, access, and attack vector identification	12	8	3	2	11	7	7	5	2	6	4
Cyber threats, attacks, and mitigations to control systems	8	13	5	2	12	7	9	2	2	7	5

<b>Course Topic</b>	<b>Analyze security incidents</b>	<b>Assess and manage risk</b>	<b>Communicate results</b>	<b>Develop and manage personnel</b>	<b>Identify and mitigate vulnerabilities</b>	<b>Implement security monitoring</b>	<b>Log security incidents</b>	<b>Manage process and procedures</b>	<b>Manage projects and budgets</b>	<b>Manage security operations</b>	<b>Respond to intrusions</b>
Defensive techniques and measures	4	9	3	4	11	7	4	2	1	6	5
Incident response	15	4	8	3	8	3	7	3		5	16
Manage WORKFORCE activities		4	3	9	2	2	2	4		3	1
Network security	8	8	5	1	10	11	8	4		9	6
Risk management	2	16	4	1	5	3	2	8	1	6	2
Security monitoring	6	3	5		4	13	10		1	6	4
Wireless technology	3	12	1	3	10	9	7	2	1	7	3

\*Blocks shaded red indicate training and education course domains that, based on the panelists' votes, map to the associated responsibility area.



## **Appendix K**


### **Review and Comment System Instructions**





# Appendix K

## Review and Comment System Instructions

Below are screenshots of the instructions received by public participants in the Review and Comment System and a sample module page.

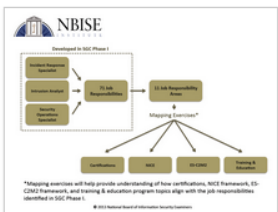
**NBISE**  
NATIONAL BOARD OF INFORMATION  
SECURITY EXAMINERS



**Pacific Northwest**  
NATIONAL LABORATORY  
*Proudly Operated by Battelle Since 1965*

**Secure Power Systems Personnel Project  
Review & Comment System**

This Review & Comment System (RaCS) is an important step toward developing a deeper understanding of the resources available to enhance the cybersecurity workforce for power systems. The RaCS allows you to provide your feedback on the results of the Smart Grid Cybersecurity (SGC) panel's efforts to map job responsibility areas to four workforce development programs for power systems cybersecurity: certifications, training & education programs, the NICE framework, and the ES-C2M2 framework. *(Click on the Mapping Diagram on the right to enlarge.)*



### RaCS Modules

This tool is divided into four review-and-comment modules, one for each Workforce Development Program. Each module consists of the results for the mapping of the selected workforce development program for your review and comment.

**Click on a button to review and comment**

[NICE Tasks](#)[ES-C2M2 Objectives](#)[Course Topics](#)[Certification Domains](#)

**To start a module:** Please click on one of the four buttons above to select a Workforce Development Program. The module for your selected workforce development program will take less than 30 minutes to complete. The directions for the module will be at the top of the module page.

### Description of Workforce Development Programs

**NICE Tasks:** The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS), is working to establish an operational, sustainable, and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security. The goal is to define cybersecurity jobs, attraction, recruitment, retention, and career path strategies.

**ES-C2M2 Objectives:** Energy Systems Cybersecurity Capability Maturity Model (ES-C2M2) is a common model that evaluates cybersecurity capabilities within the electricity sector and measures how those capabilities mature over time. This framework enables utilities to prioritize actions and investments to improve cybersecurity with a dedicated measure for workforce development.

**Course Topics:** Training and education courses focused on cybersecurity of industrial control systems and/or power systems

**Certification Domains:** Vendor-neutral certifications that were deemed 'valuable' by the SGC panel for power systems cybersecurity

For more info and support: please contact [thomas.vanderhorst@nbise.org](mailto:thomas.vanderhorst@nbise.org) so that we may assist you.

### Your privacy

This review and comment system is anonymous. The record kept of your module responses does not contain any identifying information about you unless a specific question in the module has asked for this. If you have responded to a module that used an identifying token to allow you to access the module, you can rest assured that the identifying token is not kept with your responses. It is managed in a separate database, and will only be updated to indicate that you have (or haven't) completed this module. There is no way of matching identification tokens with module responses in this review and comment system.

## Review and Comment on NICE Tasks

This activity is specifically looking at cybersecurity concerns as they relate to **power systems**. For each NICE Task row on left of the screen, review the list of selected Responsibility Areas on right. **The checkboxes with checkmarks in them** indicate areas that a focus group of subject matter experts believe are related to the NICE Task shown on the left.

If you agree that the checked Responsibility Areas are related to the NICE Task on the left, proceed to review the next row. Otherwise select/deselect the checkbox for any or all Responsibility Areas that you believe should be related to that NICE Task.

You may also provide comments about the Responsibilities related to that NICE Task by clicking on the 'Add a Comment' button under the NICE Task.

If you would like to provide a general comment on this module, click the 'Add a general comment' button at the bottom of the page.

**When you have completed your review of this module, be sure to click "SUBMIT YOUR REVIEW" at the bottom of the page to save your responses.**

### NICE Task

Assist in the construction of signatures which can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise [NICE Task ID: 427]

[Add a Comment](#)

### Responsibility Areas

Select all Responsibility Areas to which this NICE Task belongs.

- ☒ Analyze security incidents
- ☐ Assess and manage risk
- ☐ Communicate results
- ☐ Develop and manage personnel
- ☒ Identify and mitigate vulnerabilities
- ☐ Implement security monitoring
- ☐ Log security incidents
- ☐ Manage process and procedures
- ☐ Manage projects and budgets
- ☐ Manage security operations
- ☐ Respond to intrusions

Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources [NICE Task ID: 433]

[Add a Comment](#)

Select all Responsibility Areas to which this NICE Task belongs.

- ☒ Analyze security incidents
- ☐ Assess and manage risk
- ☐ Communicate results
- ☐ Develop and manage personnel
- ☒ Identify and mitigate vulnerabilities
- ☐ Implement security monitoring
- ☒ Log security incidents
- ☐ Manage process and procedures
- ☐ Manage projects and budgets

## **Appendix L**

### **Panel Votes Assigning Job Responsibilities to Job Roles**



## Appendix L

### Panel Votes Assigning Job Responsibilities to Job Roles

	Cyber Secure Power Engineer	Incident Response Specialist	Intrusion Analyst	Security Operations Specialist
<b>Job Responsibilities from Phase 1</b>				
Ensure a baseline of normal/expected activity is available or can be quickly assembled to support analysis	9	8	13	12
Ensure adequate and representative environments exist to train staff and evaluate threats and vulnerabilities and mitigations	3	2	4	5
Ensure adequate budget has been apportioned for monitoring solution	2	1	3	6
Ensure all appropriate parties are consulted and support security tool implementation	9	5	4	10
Ensure all data and evidence associated with intrusions are stored in an appropriate manner	7	13	14	10
Ensure all functional requirements meet current needs and identify tools that fall short	10	4	7	8
Ensure all incidents are classified into categories and provide data back to stakeholders, management, and risk assessment process	6	12	12	10
Ensure all internal experts and responsible parties are consulted and engaged to analyze security incidents	7	9	8	9
Ensure all intrusions are contained properly	6	14	13	9
Ensure all intrusions are eradicated or cleaned to the greatest extent possible	4	13	12	8
Ensure all open intrusions are managed in a timely manner	4	13	14	6
Ensure all operations and response activities are prioritized by Business Impact Assessment results	5	5	3	7
Ensure all security events have been identified	6	13	12	11
Ensure all security incident reporting requirements are satisfied properly	4	13	10	10
Ensure all security information regarding exposure, threats, and protective measures is provided to develop appropriate risk picture	6	8	9	10
Ensure all security operations staff and stakeholders maintain an understanding of applicable vulnerabilities and threats	7	6	4	10
Ensure all security projects are managed for budget, progress, and risk	1	2	0	6
Ensure all solutions being installed have been authorized.	8	4	3	11
Ensure all stakeholders are identified and contact information is available to determine reporting requirements and make reports	7	8	6	9
Ensure all training scenarios are current and match your organization's attack technique table	5	3	5	6
Ensure all vulnerabilities are tracked and mitigated in a timely manner	8	6	8	7

<b>Job Responsibilities from Phase 1</b>	<b>Cyber Secure Power Engineer</b>	<b>Incident Response Specialist</b>	<b>Intrusion Analyst</b>	<b>Security Operations Specialist</b>
Ensure all vulnerability and assessment findings are prioritized according to risk	6	5	8	7
Ensure appropriate stakeholders and security management receive security metrics	7	3	4	9
Ensure budget is built into role to adequately address skill set improvement, training and certifications	1	2	0	6
Ensure communication plans are updated	4	6	5	9
Ensure company policies and procedures are followed for configuration management	8	4	4	8
Ensure company policies and procedures are followed for downloading and installing third-party software	6	4	4	7
Ensure false positives are tracked, provide advice for future filtering and close ticket	5	10	10	9
Ensure hardening of operating system, services, and applications on custom or third-party solutions	11	2	4	9
Ensure incident data is collected, analyzed, maintained, and reviewed	7	13	12	8
Ensure incident response and recovery procedures are tested regularly	2	14	8	6
Ensure independent review of installation of security monitoring solutions to assess effectiveness and coverage	4	1	5	8
Ensure intrusions are closed by verifying incident response actions and testing targeted environment for additional attacker activity	5	10	13	9
Ensure incident response (IR) Specialist has been trained and current in latest threats analysis	2	10	7	4
Ensure log sources are time-synced to a local NTP server	6	4	7	8
Ensure logging and security information is stored for analysis for an appropriate period of time	5	10	9	11
Ensure maintenance of security profiles for smart grid components	8	2	2	11
Ensure maintenance of an accurate picture of utility systems deployed, architectures, communication protocols employed and business functions and processes	10	4	3	7
Ensure models exists to assess security risk	6	3	3	6
Ensure monitoring can be automated or scripted	7	4	5	8
Ensure monitoring of security state of your organization's systems and assets	8	5	6	11
Ensure monitoring solution is configured correctly to obtain vendor software and signature updates	6	4	4	9
Ensure ongoing training with refresher courses on current and future toolsets or techniques	5	1	3	6
Ensure only authorized staff can access security tools and data	8	3	5	10
Ensure operational security staff maintains a current understanding of attack and defense TTPs	5	5	7	10



<b>Job Responsibilities from Phase 1</b>	<b>Cyber Secure Power Engineer</b>	<b>Incident Response Specialist</b>	<b>Intrusion Analyst</b>	<b>Security Operations Specialist</b>
Ensure reasonable effort and capability to test deployed assets and smart grid devices	9	3	1	5
Ensure rigor and completeness of security log and information analysis	6	8	5	6
Ensure security operations staff are proficient with security tools and understand their capabilities and constraints	2	4	0	8
Ensure security staff understands company policies and technical standards	5	3	2	6
Ensure security tools are patched and updated properly	8	4	6	11
Ensure Security Information and Event Management system is operating to expected functional and/or performance requirements	6	5	9	10
Ensure sufficient artifacts are available to make determination	3	6	9	5
Ensure system owners are aware of activities prior to performing assessments	6	0	4	9
Ensure that a methodology has been established for evaluating alert types and that those thresholds are programmed into the security monitoring solution by impact level	6	6	9	8
Ensure that all assets that require monitoring are logging to the security monitoring solution and that you are able to identify each asset that is supposed to be logging	9	6	9	8
Ensure that all employees, regardless of rank/role, are familiar with the most basic usages of office-wide security software, and know where to turn if an issue arises	2	3	2	8
Ensure that personnel responsible for investigating security events understand what constitutes an actual event	6	9	10	7
Ensure that security event types have been defined by classification; for example, unauthorized access attempts to a firewall may not be considered an incident, unless they meet a certain threshold (five attempts to the firewall may not be an incident, but 5000 attempts from the same IP address may be an indication of a DoS attack)	7	8	13	6
Ensure that smart grid security components are put through an annual vulnerability assessment so that weaknesses can be identified	7	2	5	7
Ensure that you are receiving notifications from vendors in the case where they have been breached and maintain access to your networks	8	7	10	8
Ensure that you are monitoring security threat websites so that you are getting vulnerability information about assets that are in place in your network and whether or not vendors have released patches or firmware upgrades to correct those security issues	7	5	9	9
Ensure that you communicate with vendors who make your smart grid components and request that they provide you with information related to vulnerabilities that they identify	9	3	7	9
Ensure that you have set up your vulnerability scanning solution to routinely scan and identify assets for vulnerabilities	8	4	7	7
Ensure the incident response procedure/plan is executed and followed	5	12	7	7

	Cyber Secure Power Engineer	Incident Response Specialist	Intrusion Analyst	Security Operations Specialist
<b>Job Responsibilities from Phase 1</b>				
Ensure the organization conducts “lessons learned” with every material incident	4	8	8	7
Ensure the organization maintains an attack technique table with detailed TTPs	4	6	10	6
Ensure the security monitoring solution satisfies all organizational monitoring requirements	7	6	6	8
Ensure vendors are contractually notifying you of exposures and security issues of interest—a nondisclosure agreement will usually be required for full transparency	7	3	3	7
Ensure vulnerability assessment solution is configured to provide the desired results	7	3	8	9
Ensure vulnerability scanner is tested adequately to operate in the target environment	7	3	8	8
Ensure you understand application, operating systems and infrastructure to identify which tools best mitigate business risks	10	4	9	9

## **Appendix M**

### **Education and Training Courses Identified in Open Source Search**



## Appendix M

### Education and Training Courses Identified in Open Source Search

Organization	Course
Cybatl (also CNS 466 course at DePaul University)	Critical Infrastructure and Control System Cybersecurity
DePaul University	CNS 466: Critical Infrastructure and Control Systems Cybersecurity
DOE-INL	Introductory SCADA Security
DOE-INL	Intermediate SCADA Security
DOE-INL	Advanced SCADA Security Red/Blue Team
EnergySec	ICS 224: Security and Compliance: Building Programs That Achieve Both Disciplines in the Critical Infrastructure and Key Resource (CI/KR) Sectors
InfoSec Institute	SEC-325 SCADA Security
ISA	TS-13: Advanced Industrial Cybersecurity
ISA	IC32E: Cyber Security for Automation, Control, and SCADA Systems
Pennsylvania State University	CSE598e: Critical Infrastructure Security
Red Tiger Security	SCADA Security Advanced
SANS	HOSTED: Pentesting Smart Grid and SCADA
SEL University (Sweitzer Engineering Labs)	COM 203: SEL Cybersecurity Best Practices for Critical Infrastructure
Telematix Institute	SCADA Security Challenges and Solutions
Texas A&M University	ECEN 689 Cyber Security of the Smart Grid
Tonex	Course 1450: Advanced SCADA Training (Level II)
Tonex	Course 1499: SCADA Training
University of Kansas	Cybersecurity for Industrial Automation and Control Systems Online Certificate Course
University of Washington	IPM 509: Communications and Cyber Infrastructure Systems
USCERT	Cyber Security for Control Systems Engineers & Operators
USCERT	Introduction to Control Systems Cybersecurity (101)
USCERT	Intermediate Cybersecurity for Industrial Control Systems (201)
USCERT	Intermediate Cybersecurity for Industrial Control Systems (202)
USCERT	ICS Advanced Cybersecurity (301) (also DOE-INL Advanced SCADA Security Red/Blue Team)
Worcester Polytechnic Institute	Power Systems Certificate
Florida Atlantic University	EEL 5394: Cyber Security for Smart Grid
Francis Tuttle Technology Center	Cyber Security for SCADA Systems
Red Tiger Security	Blackhat SCADA Training
SANS	MGT405: Critical Infrastructure Protection
University of Houston	ELET 4311: Computer-Based Communications and Security Issues for Electrical Power Systems
University of Houston	ELET 4317: Computer-Based Electrical System Protection and Safety
USCERT	OPSEC for Control Systems
USCERT	ICS Security for Management (111)

\*The courses in RED were not included in the analysis as we were unable to find course objectives or a syllabus for these courses.



*Proudly Operated by **Battelle** Since 1965*

902 Battelle Boulevard  
P.O. Box 999  
Richland, WA 99352  
1-888-375-PNNL (7665)  
[www.pnnl.gov](http://www.pnnl.gov)



U.S. DEPARTMENT OF  
**ENERGY**