Carnegie Mellon University
Software Engineering Institute

NICE Framework Cybersecurity Evaluator

Christopher Herr

August 2020

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-0279

Table of Contents

List of Figures

List of Tables

Abstract

The Software Engineering Institute (SEI), in partnership with the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), researched, designed, and developed a Cybersecurity Evaluator with the goal of assessing potential and current members of the cyber workforce within the scope of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework). Initial research was conducted to ascertain how Knowledge, Skills, and Abilities (KSAs) aligned across the NICE Framework within their respective Categories, Specialty Areas and Work Roles. By identifying overlapping KSAs, the SEI discovered that a Cybersecurity Evaluator tool could provide a reasonable baseline assessment using just 65 questions, which target approximately 28% of the key KSAs within the NICE Framework. Assessment results will help an individual identify the NICE Category and potential roles that best align to their current talents and strengths.

1 NICE Framework Frequency Analysis

Initial Research and Frequency Analysis

Initial research was performed to better understand the NICE Framework and the ways in which the many KSAs overlapped across the numerous Work Roles. While the NICE Framework describes the possible Knowledge, Skills, and Abilities that a person may need in order to perform in a role, it seems unrealistic that a member performing each role would exhibit 100% of the KSAs tied to that role. Therefore, analysis was aimed at determining the most applicable or most critical KSAs to assess in the Cybersecurity Evaluator.

Frequency analysis was conducted on the NICE Framework to determine which KSAs were the most commonly used across all Work Roles.

Our original hypothesis was:

> Incorporating a set of top-tiered KSAs into the Cybersecurity Evaluator would provide a valuable overall assessment that could evaluate users across the entire NICE Framework to determine strengths within the various Categories, Specialty Areas and Work Roles. These top KSAs would inherently be more generic and high level, making for better general aptitude questions in the first assessment by addressing foundational cybersecurity knowledge.

The result was:

> Assessing the most common KSAs (or the top 100) would provide coverage upwards of 40% of the total number of KSA instances in all 52 Work Roles. The majority of these KSAs tended to be Knowledge.

For the purpose of this paper:

- Coverage is defined as the [# of instances per KSA statement for the top 100 KSAs in the Framework] / [# of instances per KSA statement for all 52 Work Roles in the Framework].
- There are roughly ~1083 unique KSAs in the Framework[1]
- The total number of instances per KSA statement for all 52 Work Roles is ~3258.
- The top 100 most common KSAs provide a ~37.91% coverage rate (1235) of the ~3258 total instances.
- Note that as the Framework evolves, these specific numbers may also change.

[1] not counting KSAs that have been withdrawn or have 0 instances per statement

Table 1: Table of "Top 100" KSAs

KSA #	Work Role Instances per Statement	KSA #	Work Role Instances per Statement	KSA #	Work Role Instances per Statement	KSA #	Instances per Statement	KSA #	Work Role Instances per Statement
K0001	52	K0070	13	K0146	10	K0048	8	K0042	7
K0002	52	K0624	13	K0203	10	K0049	8	K0043	7
K0003	52	A0089	13	K0322	10	K0093	8	K0072	7
K0004	52	K0036	12	K0395	10	K0101	8	K0082	7
K0005	52	K0059	12	K0417	10	K0139	8	K0102	7
K0006	52	K0170	12	K0516	10	K0267	8	K0154	7
K0179	19	K0177	12	K0560	10	K0342	8	K0167	7
K0287	18	A0066	12	K0021	9	K0349	8	K0377	7
K0261	17	K0056	11	K0027	9	K0427	8	K0379	7
K0262	17	K0061	11	K0180	9	K0436	8	K0449	7
K0260	16	K0108	11	K0362	9	K0440	8	K0610	7
K0109	15	K0168	11	K0392	9	K0446	8	K0614	7
K0044	14	K0200	11	K0445	9	K0480	8	S0027	7
K0126	14	K0431	11	K0471	9	K0499	8	S0060	7
K0169	14	K0444	11	S0296	9	K0561	8	S0297	7
K0332	14	K0565	11	A0070	9	K0612	8	A0082	7
S0367	14	A0170	11	A0085	9	S0218	8	A0084	7
A0013	14	K0018	10	A0106	9	S0249	8	A0105	7
A0123	14	K0058	10	K0019	8	A0015	8	K0009*	6
K0060	13	K0090	10	K0028	8	K0024	7	K0015*	6
								Total	**1235**

* There are several KSAs with six instances per statement and these two serve only as examples within the top 100.

2 Cybersecurity Evaluator Design

Generalized Aptitude Assessment

The frequency analysis research above was used to create the generalized aptitude assessment that evaluates the user across the NICE Framework, identifies general talent and recommends potential strength areas, ranked by performance. This high-level assessment is inherently more knowledge based rather than skill or ability based. A breakdown of the final KSA to assessment mapping can be found in Table 2.

General Aptitude Assessment Question Development

The number of questions the assessment asks was kept small (65) to reduce the amount of time it takes to complete the assessment and also to make the material covered more manageable. At 65 questions, the assessment should take the average user no more than one hour.

Ultimately, one question was written for each KSA in the assessment that attempts to get to the core of its description. For example:

> Ability ID: A0101
>
> Ability Description: Ability to recognize and mitigate cognitive biases which may affect analysis.
>
> Question: Match the following types of cognitive bias with the appropriate definition.

Of the top 100 most frequent KSAs in the Framework:

> 81 were Knowledge
>
> 7 were Skills
>
> 12 were Abilities

Knowledge-based KSAs were the most straight forward to be assessed by a question. Some skills and abilities could be assessed by a question, or could be folded into a Knowledge-based question of a similar kind.

The original 100 KSA count was reduced to 60 due to the nature of some of the descriptions and the difficulty in translating many of those to a single question-based assessment (such as “Ability to interpret and understand complex and rapidly evolving concepts”). As the more difficult to measure KSAs were omitted, other more common and easily measurable ones were moved up to replace them until a pool of 60 was formed. This pool of 60 questions then represents the most common Framework KSAs, which are also the most straight forward to assess by a single question.

Five additional knowledge questions specific to the Investigate category were subsequently added to more equally represent its somewhat isolated and unique KSA set, bringing the total number of questions to 65.

The final assessment consists of questions related to 49 Knowledge, 14 Skills, and 2 Abilities with overlapping of five similar KSAs included.

Table 2: Table of KSAs Assessed

K0001	K0002	K0003	K0004	K0005	K0006	K0009*	K0018	K0036	K0043
K0044	K0050	K0052	K0056	K0058	K0059	K0060	K0061	K0063	K0070
K0077**	K0090	K0108	K0109	K0123**	K0126	K0128**	K0145**	K0146	K0155**
K0168	K0169*	K0170	K0177	K0179	K0200	K0203	K0260	K0261	K0262
K0287	K0322	K0332	K0395	K0417	K0431	K0444	K0516	K0560	K0565
K0624	S0001	S0022	S0031	S0038	S0060	S0073	S0174	S0175	S0184
S0249	S0250	S0285	S0289	S0367	A0001*	A0015*	A0101	A0106	A0123*

* Denotes a secondary KSA that is also assessed by another KSAs question.

** Denotes a KSA that was added in order to better represent the Investigate Category of Work Roles

Assessment Effectiveness

When the question set was reduced from 100 KSAs to 65 primary and 5 secondary KSAs, the overall coverage of the NICE Framework is roughly 27.9%: ~909 assessment KSA instances out of ~3258 total.

The assessment is heavily based on Knowledge as the most common KSA type. While the assessment includes only 51 Knowledge from the Framework, the coverage amount for Knowledge only is 37.3%: ~791 assessment Knowledge instances out of ~2119 total Knowledge instances in the Framework.

Table 3: Table of KSA Coverage

	# of Assessment KSA Instances Per Work Role	# of Framework KSA Instances Per Work Role	% Coverage within Work Role
All Source-Collection Manager	17	110	15.45%
All Source-Collection Requirements Manager	17	96	17.71%
All-Source Analyst	22	92	23.91%
Authorizing Official/Designating Representative	23	52	44.23%
Communications Security (COMSEC) Manager	10	30	33.33%
Cyber Crime Investigator	12	31	38.71%
Cyber Defense Analyst	26	91	28.57%

	# of Assessment KSA Instances Per Work Role	# of Framework KSA Instances Per Work Role	% Coverage within Work Role
Cyber Defense Forensics Analyst	20	70	28.57%
Cyber Defense Incident Responder	14	40	35.00%
Cyber Defense Infrastructure Support Specialist	13	34	38.24%
Cyber Instructional Curriculum Developer	11	53	20.75%
Cyber Instructor	15	92	16.30%
Cyber Intelligence Planner	17	142	11.97%
Cyber Legal Advisor	9	19	47.37%
Cyber Operator	11	74	14.86%
Cyber Ops Planner	18	111	16.22%
Cyber Policy and Strategy Planner	11	22	50.00%
Cyber Workforce Developer and Manager	9	31	29.03%
Data Analyst	10	63	15.87%
Database Administrator	12	32	37.50%
Enterprise Architect	25	68	36.76%
Executive Cyber Leadership	10	31	32.26%
Exploitation Analyst	13	81	16.05%
Information Systems Security Developer	36	89	40.45%
Information Systems Security Manager	24	59	40.68%
IT Investment/portfolio Manager	9	19	47.37%
IT Program Auditor	12	26	46.15%
IT Project Manager	14	35	40.00%
Knowledge Manager	11	27	40.74%
Law Enforcement/Counter Intelligence Forensics Analyst	18	63	28.57%
Mission Assessment Specialist	23	92	25.00%
Multi-Disciplined Language Analyst	11	79	13.92%
Network Operations Specialist	17	58	29.31%
Partner Integration Planner	14	67	20.90%
Privacy Officer/Privacy Compliance Manager	7	28	25.00%
Product Support Manager	13	34	38.24%
Program Manager	12	32	37.50%
Research and Development Specialist	14	43	32.56%
Secure Software Assessor	24	57	42.11%
Security Architect	29	100	29.00%
Security Control Assessor	39	168	23.21%
Software Developer	26	63	41.27%
System Administrator	14	45	31.11%
Systems Developer	33	79	41.77%
Systems Requirements Planner	24	58	41.38%

	# of Assessment KSA Instances Per Work Role	# of Framework KSA Instances Per Work Role	% Coverage within Work Role
Systems Security Analyst	27	57	47.37%
Systems Testing and Evaluation Specialist	20	47	42.55%
Target Developer	23	108	21.30%
Target Network Analyst	15	95	15.79%
Technical Support Specialist	11	33	33.33%
Threat/Warning Analyst	23	80	28.75%
Vulnerability Assessment Analyst	21	51	41.18%
Overall Average	909	3258*	27.87%
Average Count | Overall Coverage | Coverage Average per Work Role	17.48	27.90%	31.45%

* There was a tiny discrepancy of 1 KSA instance between the total # of instances and the sum of all Work Role KSA instances within the data provided by NICE. In order to err on the side of caution, we based our statistical analysis off of the higher of the two values.

Scoring and Reporting

Each question of the assessment relates to a single KSA, except in cases where two were so similar they could both be covered by the same question. Each primary KSA was mapped to its corresponding Categories and Work Roles (secondary KSAs were ignored for scoring purposes and are only included when determining coverage of the Framework).

A weighted scoring mechanism for each question works in the following way:

> If the KSA for a question applies to four roles in category A, one role in category B, and two roles in category C, then a user would receive four points in category A, one point in category B, and two points in category C when answering the question correctly. If answered incorrectly, the user receives 0 points.

In this manner, questions and KSAs that relate to more roles than another are weighted higher within the assessment. They are also weighted higher within the Categories when they apply to more work roles. Since the score for each Category is only measured within itself, the percentage scored in one Category is still relative to the others.

The overall score report at the end of the assessment is:

- [# of points scored in the Analyze category] / [# of total points possible in the Analyze category]
- [# of points scored in the Collect and Operate category] / [# of total points possible in the Collect and Operate category]
- [# of points scored in the Investigate category] / [# of total points possible in the Investigate category]
- [# of points scored in the Operate and Maintain category] / [# of total points possible in the Operate and Maintain category]
- [# of points scored in the Oversee and Govern category] / [# of total points possible in the Oversee and Govern category]

- [# of points scored in the Protect and Defend category] / [# of total points possible in the Protect and Defend category]
- [# of points scored in the Securely Provision category] /[# of total points possible in the Securely Provision category]
- [# of questions answered correctly overall] / [# of questions total]

Analyze:	46.9%	61/130 Points correct
Collect and Operate:	68.8%	64/93 Points correct
Investigate:	42.9%	21/49 Points correct
Operate and Maintain:	38.6%	39/101 Points correct
Oversee and Govern:	26.1%	41/157 Points correct
Protect and Defend:	46.4%	32/69 Points correct
Securely Provision:	43.6%	116/266 Points correct
Total questions correct:	64.6%	42/65 Questions correct

Figure 1: Score Report

The benefit of these results is to compare talent or strength in one Category versus the others. The Category(ies) with the highest score are the Category(ies) where the user has the most strength. This information can help guide career path decisions. Inversely, if a user desires to pursue a specific career path in a Category where they did not score well, they may wish to complete further education and training in those areas. The goal of the assessment is not to score 100% overall, but to achieve and recognize relative strengths in each Category.

Delivery Methods

The Cybersecurity Evaluator can be offered in one of two ways:

- The Cybersecurity Evaluator can be hosted directly within a webpage or website and run in the user's web browser. All files must be included in the web root directory for the tool to run properly.
- The Cybersecurity Evaluator can be made available as a downloadable package to be run locally on a user's system. Once unpackaged, it can be run in any modern web browser but does not require an Internet connection.

Execution of the Assessment

Questions are matching, multiple-choice, multiple-select, fill-in-the-blank, and survey type questions.

Users are able to review the individual question results following completion of the assessment.

To get an honest assessment, users should not perform external research to answer questions or blindly guess at questions they cannot answer. Doing either would skew the results and provide a less accurate true score.

Assessment Metrics

Question Numbers by Category

Of the 65 primary KSAs in the assessment, the number of questions per category and possible points are as follows:

- 25 questions related to the Analyze Category (130 points possible)
- 21 questions related to the Collect and Operate Category (93 points possible) 19 questions related to the Investigate Category (49 points possible)
- 32 questions related to the Operate and Maintain Category (101 points possible) 33 questions related to the Oversee and Govern Category (157 points possible) 28 questions related to the Protect and Defend Category (69 points possible)
- 50 questions related to the Securely Provision Category[2] (266 points possible)

The ratio of points per category is roughly in line with the ratio of work roles per category for the Framework.

Table 4: Points and Role Ratios

	Analyze	Collect and Operate	Investigate	Operate and Maintain	Oversee and Govern	Protect and Defend	Securely Provision	Totals
Total Points per Category	130	93	49	101	157	69	266	**865**
Points Ratio per Assessment	14.98%	10.71%	5.65%	11.64%	18.09%	7.95%	30.65%	**100%**
Work Roles per Category	7	6	3	7	14	4	11	**52**
Ratio of Work Roles in Framework	13.46%	11.54%	5.77%	13.46%	26.92%	7.69%	21.15%	**100%**

Of the seven Categories, the ratio of points for Analyze, Collect and Operate, Investigate, Operate and Maintain, and Protect and Defend all fall within 2% of their ratio of roles in the Framework. Oversee and Govern is somewhat under represented, due to the high level of soft skills and

[2] Securely Provision is the most highly represented Category, likely because software and system development relies heavily on understanding many facets of cybersecurity.

abilities that are not included in the assessment. Securely Provision is slightly over represented due to it involving many (50) of the assessment KSAs in multiple roles.

Work Role Counts

Count is simply the number of times an assessment question applies to a Work Role.

The five Work Roles that are referenced the most by count are:

1. Security Control Assessor[3] (SP) - 39
2. Information Systems Security Developer (SP) - 36
3. Systems Developer (SP) - 33
4. Security Architect (SP) - 29
5. Systems Security Analyst (OV) - 27

The five Work Roles that are referenced the least **by count** are:

1. Privacy Officer/Privacy Compliance Manager (OV) - 7
2. Cyber Legal Advisor4 (OV) - 9
3. Cyber Workforce Developer and Manager (OV) - 9
4. IT Investment/Portfolio Manager4 (OV) - 9
5. COMSEC Manager (OV) - 10

Work Role Coverage

Coverage is count divided by the total number of KSAs that apply to a Work Role.

The five Work Roles with the highest amount of **coverage** are:

1. Cyber Policy and Strategy Planner (OV) - 50.00%
2. Systems Security Analyst (OM) - 47.47%
3. IT Investment Portfolio Manager4 (OV) - 47.37%
4. Cyber Legal Advisor4 (OV) - 47.37%
5. IT Program Auditor (OV) - 46.15

The five Work Roles with the lowest amount of **coverage** are:

1. Cyber Intelligence Planner (CO) - 11.95%
2. Multi-disciplined Language Analyst (AN) - 13.92%
3. Cyber Operator (CO) - 14.86%
4. All Source-Collection Manager (CO) - 15.45%
5. Target Network Analyst (AN) - 15.79%

---

[3] Security Control Assessor also references the most KSAs of any Work Role in the Framework with 168 KSAs referenced, so this high count value only represents less than 40% of the Work Roles KSAs

[4] IT Investment Portfolio Manager and Cyber Legal Advisor have low counts and high coverage due to the small number of KSAs that they include (19) and the number of times they are referenced by a KSA/question in the assessment (9).

The average number of KSA references per Work Role in the assessment was ~17.48 and the average coverage per Work Role was ~31.45%. (See Table 3.)

3 Challenges

Work Roles vs KSAs

For each Work Role, there is a set of related KSAs that a person might be required to have. However, it is unlikely that a person in a role would exhibit all of the KSAs within that role, especially when the role requires a very large number of KSAs. Would a person need to be tested on *all* of the KSAs listed within a role to be deemed proficient? If not, what is the cutoff? This was why the SEI decided to focus on the most common KSAs across the Framework instead of focusing on KSAs that are very specific to individual roles.

Tasks vs KSAs

Another challenge with the Framework is that there is no direct mapping of Tasks to the corresponding Knowledge, Skills, or Abilities required to perform those Tasks. To develop assessments and training that evaluate a user's ability to perform job duties and Framework Tasks, understanding what those Tasks entail (and what the prerequisite KSAs are to perform them) is essential. Lacking this mapping, the trainer or developer can match the few KSAs and Tasks with similar descriptions to each other. Otherwise, a trainer or developer must conduct keyword searches and analysis of the KSA descriptions within a Work Role and apply them to the necessary Tasks in a logical manner. This mapping of KSAs to Tasks is critical in order to reliably measure a user's ability to perform Tasks while also demonstrating proficiency in the required KSAs.

Assessing Skills and Abilities

Addressing some Framework Skills and Abilities often requires the user to demonstrate them through some sort of hands-on assessment. Other Framework Skills and Abilities are somewhat subjective or relate highly to personal or soft skills – not something that can be so simply asked or tested. Examples include: effective writing, effective communication, and presentation skills. Other KSAs reference what a person should know or be able to do, but the Framework does not describe how a person would demonstrate such skills and abilities. Because Tasks are not directly mapped to KSAs within a role, it is hard to determine what a user would do to demonstrate proficiency in a specific KSA or accomplish a specific task with those skills or abilities.

Proficiency Levels

While the Framework does define what the expected education, training, experience, and certifications or credentials are for the Entry, Intermediate, and Advanced levels for each Work Role, there is no mapping of which KSAs or Tasks are required at each level. Is it expected that an Expert level member of a role has 90-100% of the related KSA experience and can perform 90-100% of the necessary Tasks? Are those KSAs and Tasks evolving or fluctuating as the member advances in proficiency? It is unfair to test everyone at a higher level. Instead, it is ideal to assess

everyone at the lowest level first, and then direct the member to further assessments for those higher proficiency levels.

Performance Based Assessments

The SEI developed a prototype hands-on performance-based assessment using the Cyber Defense Forensics Analyst Work Role. Due to the technical nature of this specific role and the subject matter of the training content, finding applicable KSAs and Tasks was rather straight forward.

As an example, a performance-based assessment that was focused on hard disk analysis was able to be mapped in the following manner:

> Learning Objectives
>
> By the end of this lab you will be able to:
>
> - Generate a timeline based on the webserver compromise
>
> **T0287 – Perform static analysis to mount an image of a drive**
>
> **T0396 – Process image with appropriate tools depending on analyst's goals**
>
> - Successfully load the hard drive evidence item in FTK for analysis
>
> **T0287 – Perform static analysis to mount an image of a drive**
>
> **T0396 – Process image with appropriate tools depending on analyst's goals**
>
> - Analyze a registry for suspicious items
>
> **T0397 – Perform Windows registry analysis**
>
> - Analyze a hard drive image using FTK
>
> **T0286 – Perform file system forensic analysis**
>
> - Analyze a timeline for known events
>
> **T0173 – Perform timeline analysis**
>
> Overall Lab Objectives
>
> **T0027: Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.**
>
> **T0036: Confirm what is known about an intrusion and discover**

Additional hands-on labs on the subject could be easily mapped to additional KSAs and Tasks within the Cyber Defense Forensic Analysts Work Role, including objectives on memory analysis, packet-capture analysis, understanding and analysis of volatile system data, and more. Assessments of each KSA or Task could also be made by using quizzes or by interrogating the system for state data, commands histories, or existence of specific data.

Objective: Analyze the volatility output files in order to determine four key pieces of information for the case. (Quiz)

S0091: Skill in analyzing volatile data

T0532: Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information

Objective: Extract seven specific pieces of information from the memory file and analyze them to further the case (System interrogates output files for correct size and length, quiz)

S0062: Skill in analyzing memory dumps to extract information

Objective: Load the packet capture or penregsiter file into Wireshark and analyze the capture for further information about the suspect's activities (Quiz)

K0301: Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).

S0156: Skill in performing packet-level analysis.

T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.

Through this mapping process it became very clear that even when assessing a small portion of KSAs and Tasks, the amount of time spent by the user to complete the assessment could be significant. This ties back to the original challenge of understanding the Framework and what it means to be in a Work Role. In order to physically assess many Tasks and KSAs it would take an increasingly large amount of time, depending on the role. Some roles (Cyber Legal Advisor) are small, having just 19 related KSAs and 13 related Tasks, though the tasks are very involved with legal proceedings. Other roles are much broader in scope. For example, the Privacy Officer/Privacy Compliance Manager role includes 72 Tasks, while the Security Control Assessor role includes 168 KSAs. Either one of these Work Roles would require extensive time to assess fully based purely on the number of Tasks and KSAs required. Not all roles could be handled in the same amount of time, making some assessments take longer to develop and assess.

Finally, as there is no mapping of KSAs to Tasks, or proficiency levels defined by KSAs or Tasks, it is difficult to know what makes for a good representation to assess each role at each proficiency level and what is truly required by each role. The NICE Framework is a great starting point, but future research into the educational levels or required certifications for each proficiency level (including interviews and surveys of personnel working in these roles) would provide valuable information to better develop viable performance-based assessments that would be more accurate and complete within the Framework.

4 Summary

The Cybersecurity Evaluator was created to be a fairly robust and generalized tool for assessing one's knowledge, skills, and abilities within the NICE Framework. The Evaluator is simple to distribute and requires no additional software to run, other than a modern web browser.

Results can be used to highlight strengths in various cybersecurity career areas or talent gaps that should be filled before pursuing a particular career path. There are many challenges when creating assessments, whether knowledge or performance based. Doing so within the NICE Framework is no exception. However, based on the research and frequency analysis performed, the Cybersecurity Evaluator stands as a valuable tool for one to identify talent, evaluate aptitude, and assess expertise within the NICE Framework.