N2K

women in CYBERSECURITY WiCyS

CYBER TALENT STUDY

2024

TABLE OF CONTENTS

Executive Summary 3
- Key Takeaways 4

Introduction 5
- The Participants 5
- Our Approach 6

WiCyS Members Out-Perform 8
- Superior Performance 9
- Opportunities for Development 9

WiCyS Member Excellence in N2K Functional Groups 10
- Communications & Network Security 11
- Cyber Workforce Training & Awareness 12
- Cyber/IT Leadership & Management 13
- Cyber/IT Policy & GRC 14

WiCyS Strategic Initiatives 16

Opportunities for Growth & Partnership 17

Closing Insights 18

Additional Resources 19

"As a participant, I'm deeply grateful to both WiCyS and N2K. Understanding my strengths and weaknesses helped me chart a clearer path in my cybersecurity career. Additionally, the free courses provided essential knowledge to enhance my abilities."

Rocelli C.
IT Technical Project Specialist,
NYC Department of Sanitation (DSNY)

EXECUTIVE SUMMARY

The collaboration between N2K Networks Inc. (N2K) and Women in CyberSecurity (WiCyS) represents a strategic fusion of expertise and advocacy designed to advance and diversify the cybersecurity workforce. This report leverages N2K's analytical strengths to map WiCyS members' skills directly to the NICE Workforce Framework, categorizing capabilities into functional areas that highlight the unique strengths and potential growth opportunities for WiCyS members. By conducting thorough diagnostics and focused analyses, this partnership identifies the capabilities of WiCyS members and aligns them with industry standards to ensure that their skills are recognized and utilized to the fullest. N2K and WiCyS are setting new benchmarks in professional development and industry readiness by fostering an environment that enhances cybersecurity skills.

The findings from this collaboration highlight the exceptional skills of WiCyS members across various areas of the N2K Functional Areas, which are mapped to the NICE Framework.

HIGHLIGHTED ACHIEVEMENTS

OUTPERFORMING IN **17/20** OF THE SPECIALTY AREAS ASSESSED

Areas of Strength:

Communications & Network Security

60.6%

Cyber Workforce, Training & Awareness

62.3%

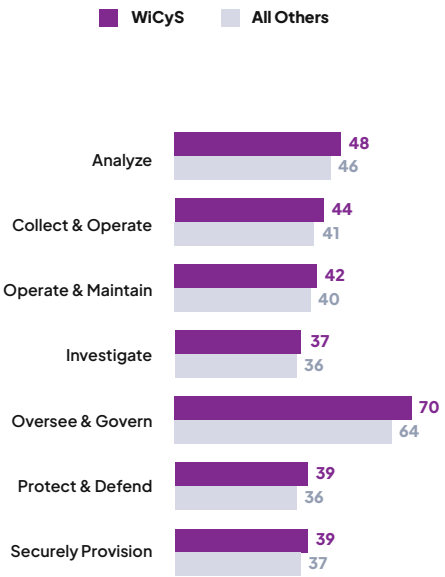
Cyber/IT Leadership & Management

64%

Cyber/IT Policy & Governance

64.3%

OUTPERFORMING IN **EVERY** NICE CATEGORY:

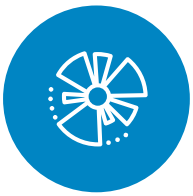


KEY TAKEAWAYS

These results demonstrate the effectiveness of WiCyS educational programs in nurturing highly skilled professionals and reinforcing the organization's role in contributing thought leadership and innovation within the cybersecurity industry. The performance of WiCyS members in these assessments underscores the potential and capability of its members in cybersecurity, affirming WiCyS's pivotal role in shaping the cybersecurity industry's future.

Outstanding Performance

WiCyS members have demonstrated exceptional performance across several key areas of the NICE Framework, underscoring the importance of WiCyS's training and development programs.



Strategic Insights

Analysis revealed remarkable strengths and areas for development, providing WiCyS with actionable data to tailor future programs and initiatives and ensure its members remain at the forefront of cybersecurity excellence.

Actionable Insights for Cybersecurity Workforce Development

The study revealed critical areas for targeted development to enhance cybersecurity workforce readiness. This insight empowers WiCyS to tailor its programs specifically to meet the diverse needs of its members, ensuring all participants are prepared to take on significant roles and lead in the cybersecurity industry.

Leadership Readiness Among WiCyS Members

The study highlights that WiCyS members are highly skilled and uniquely prepared for leadership roles within the cybersecurity industry. Their exceptional performance across critical NICE Framework functional areas demonstrates their readiness to lead and influence at high levels. These capabilities position WiCyS members as prime candidates for advancing cybersecurity initiatives and shaping future industry standards.

Proven Expertise in Critical Cybersecurity Domains

The data show the outstanding capabilities of WiCyS members within the cybersecurity landscape. Excelling in nearly every N2K Functional Area mapped to the NICE Framework, WiCyS members have shown they not only meet but exceed the standards in key domains, including Communications & Network Security, Cyber Workforce, Training & Awareness, Cyber/IT Leadership & Management, and Cyber/IT Policy & Governance, Risk and Compliance (GRC). Their scores illustrate a readiness to tackle complex challenges and lead innovations within the cybersecurity field.

INTRODUCTION

In the fall of 2023, WiCyS and N2K formalized a partnership designed to provide insights into the state of cybersecurity talent across the WiCyS organization.

The partnership between N2K Networks Inc. (N2K) and Women in CyberSecurity (WiCyS) represents a significant step forward in boosting skills and fostering innovation in the cybersecurity industry. This strategic partnership combines N2K's deep analytical expertise in cybersecurity workforce development alongside WiCyS's expansive network within the cybersecurity community. Together, N2K and WiCyS conducted a comprehensive analysis of WiCyS members' skills to spotlight strengths, identify skill gaps, and ultimately foster a robust and diverse cybersecurity workforce.

At the core of WiCyS is a compelling mission: to recruit, retain, and advance women in cybersecurity. Their vision is a world where the cybersecurity workforce is as inclusive as it is skilled, welcoming diverse talents and perspectives with open arms.

The primary goal of this collaboration was to conduct an in-depth analysis of WiCyS members' cybersecurity skills. This initiative was designed to uncover critical insights into WiCyS members' capabilities through diagnostic assessments and enriched by demographic data. The study explores the nuances of skill sets across various roles, pinpoints areas for development, and generates significant findings that will inform strategic enhancements in training and professional growth.

THE PARTICIPANTS

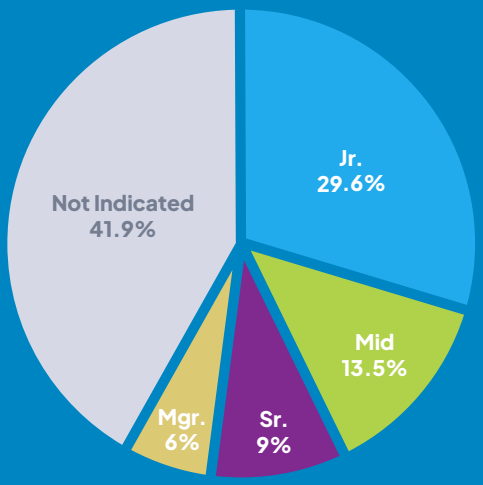
WiCyS members participating in the study represent a full range of cyber work roles and experience levels. In total, 399 members participated in the study. Because some survey data was optional for participants, 41.8% of participants did not indicate their experience level, and 27.8% opted not to indicate which functional area of cybersecurity they represented.

Total Participants:

399

Experience Levels:

- Junior: **118**
- Mid: **54**
- Senior: **36**
- Manager: **24**
- Not indicated: **167**



N2K Functional Groups:

- Analysis: **33**
- Communications & Network Security: **11**
- Cyber Workforce: **24**
- Cyber/IT Leadership & Management: **17**
- Cyber/IT Policy & Governance: **63**
- Data Engineering & Analytics: **7**
- Defensive Security Operations: **34**
- Identity & Access Management: **10**
- Incident Response & Forensics: **16**
- Offensive Security Operations: **12**
- Operational Technology & Engineering: **3**
- Security Architecture & Engineering: **18**
- Security Assessments & Testing: **30**
- Software/App Security & DevSecOps: **10**
- Not Indicated: **111**

OUR APPROACH

The approach adopted for this study involved voluntary participants from WiCyS's diverse member base and following them through N2K's NICE Workforce Diagnostic, which is designed to rigorously evaluate participant knowledge and skills across various specialty areas and competency areas identified in the NICE Cybersecurity Workforce Framework. This methodical approach ensured comprehensive and precise data collection, providing a clear snapshot of the member's current capabilities and potential areas for improvement.

N2K's NICE Workforce Diagnostic is designed to measure performance against TKS (task, knowledge, and skill) statements and competencies for a variety of defined cybersecurity work roles. This method of diagnosing a workforce, along with innovative data visualizations and dashboards to analyze and compare performance data, allows N2K to identify potential strengths and gaps across a cybersecurity and cyber-enabled workforce.

Process:

Call for participation across WiCyS member base. Over 700 WiCyS members "raised their hand as willing participants."

N2K provisioned WiCyS participants access to N2K's NICE Workforce Diagnostic. Of the volunteers, 399 WiCyS members completed the diagnostic. Participating members were also given access to **N2K's Critical Knowledge Course** as a thank you for completing the diagnostic.

N2K analyzed the results of the diagnostic, using Experience Levels and N2K's Functional Groupings as key components to interpret results. Because N2K's NICE Workforce Diagnostic tests participants' knowledge and skills across the broad spectrum of the NICE Framework, it's important to analyze the results through the lens of the functions of their work roles and experience. As a result, N2K can interpret results by Experience Levels, N2K's Functional Grouping, and NICE Specialty Areas (and combinations thereof).

Analyzing & Interpreting Results:

The findings from this talent study revealed significant strengths among WiCyS members, who consistently demonstrated exceptional proficiency across most of the NICE Framework. Their performances in the NICE Specialty Areas: Legal Advice and Advocacy, Executive Cyber Leadership, Cybersecurity Management, Cyber Operational Planning, Strategic Planning, and Policy were particularly noteworthy.

These areas showcased the depth of their cybersecurity knowledge and also highlighted their potential to lead and innovate within the industry. The data also show specific opportunities for further opportunities, guiding WiCyS in refining its training and development programs to better support its members' professional growth and ensure their skills remain at the forefront of industry standards.

About the NIST–NICE Cyber Workforce Framework:

The National Initiative for Cybersecurity Education (NICE) Cyber Workforce Framework, developed by the National Institute of Standards and Technology (NIST), plays a crucial role in addressing cybersecurity education, training, and workforce development needs. By providing a standardized taxonomy and common lexicon, the NIST-NICE Cyber Workforce Framework enables organizations to define and understand the essential tasks, knowledge, and skill (TKS) statements required for cybersecurity roles. This framework not only aids in the development and training of cybersecurity professionals but also helps in workforce planning and management. Additionally, the NICE Framework establishes a taxonomy and common lexicon that describes cyber security work and workers irrespective of where or for whom the work is performed.

On March 5th, 2024, NIST unveiled the latest update to this essential framework: version 1.0.0 of the NIST-NICE Cyber Workforce Framework. This release marks a significant milestone, as it incorporates several updates aimed at refining and enhancing the framework to better align with the current and future needs of the cybersecurity workforce. As the threat landscape continues to evolve, so too must the strategies and frameworks that underpin the development of those who support cyber missions and work.

It's important to note that this Talent Inventory Study was launched prior to the March 2024 update to the NICE Framework (version 1.0.0), and therefore analyze performance results to the 2017 version of the NICE Framework, particularly to the NICE Categories and Specialty Areas as defined in that version of the Framework.

About the N2K's Functional Groups & Taxonomy:

To address industry challenges in translating various elements of the NICE Framework into common job titles and functional teams used for cyber professionals across the commercial sector, N2K established and defined 14 Functional Groups*. These groups serve as a translation taxonomy, or a "Rosetta Stone." Utilizing N2K's Functional Groups offers a streamlined way to analyze performance and interpret workforce needs, reflecting common cybersecurity team structures.

Moreover, N2K has mapped elements of the NICE Framework—such as NICE Work Roles, Specialty Areas, and Competency Areas—as well as common certifications and training programs to these Functional Groups. This mapping provides a more comprehensive picture of the cyber workforce and training ecosystem. It enables N2K to analyze and compare datasets in several unique ways, offering deeper insights into workforce dynamics and training needs.

NICE CWF

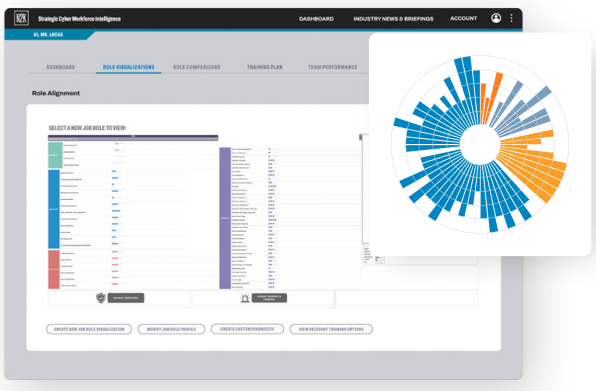
- Oversee & Govern
- Securely Provision
- Operate & Maintain
- Protect & Defend
- Investigate
- Analyze
- Collect & Operate

N2K FUNCTIONAL GROUPS

*View N2K's Functional Groups on page 5.

WiCyS EXPERIENCE LEVELS

- Junior
- Mid-Level
- Senior
- Manager
- Not Indicated

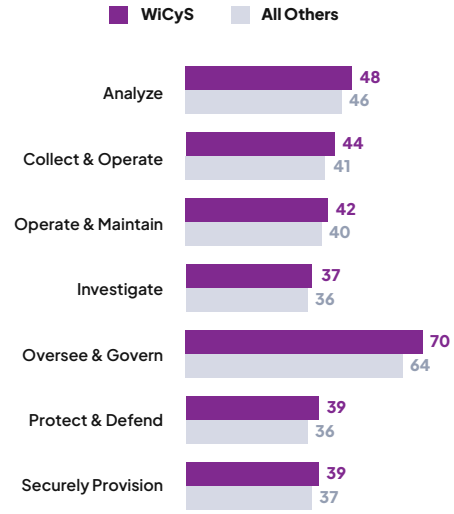


N2K'S Data Analytics & Visualization Tools to Analyze Results

WiCyS MEMBERS EXCEL ACROSS NICE CATEGORIES & MOST SPECIALTY AREAS ASSESSED

At the heart of the collaboration between N2K and Women in CyberSecurity (WiCyS) is a shared mission to highlight the remarkable professional capabilities of WiCyS members. **This section of the report analyzes the accomplishments and insights from the in-depth skills review carried out in this collaboration, aligned to the NICE Framework Categories and subsequent Specialty Areas that were included in N2K's diagnostic.**

WiCyS, with its mission to recruit, retain, and advance women in the field, plays a crucial role in shaping a diverse and dynamic cybersecurity workforce. The organization provides a wide range of training and mentoring resources, community support, and professional development programs, all designed to elevate the leadership, professional, and technical skills of all of its members.



NICE SPECIALTY AREAS	WiCyS	ALL OTHERS
AN-ASA: All Source Analysis	18	13
AN-EXP: Exploitation Analysis	34	31
AN-TGT: Targets	74	74
AN-TWA: Threat Analysis	52	51
CO-CLO: Collection Operations	28	28
CO-OPL: Cyber Operational Planning	60	54
IN-INV: Cyber Investigation	37	36
OM-NET: Network Services	45	44
OM-ADM: Systems Administration	48	41
OM-ANA: Systems Analysis	33	35
OV-MGT: Cybersecurity Management	68	66
OV-EXL: Executive Cyber Leadership	67	56
OV-LGA: Legal Advice & Advocacy	94	88
OV-SPP: Strategic Planning & Policy	53	49
PR-CDA: Cyber Defense Analysis	39	32
PR-INF: Cyber Defense Infrastructure Support	51	44
PR-CIR: Incident Response	46	48
PR-VAM: Vulnerability Assessment & Management	22	19
SP-RSK: Risk Management	53	46
SP-DEV: Software Development	25	28

SUPERIOR PERFORMANCE IN NICE SPECIALITY AREAS

The chart on page 8 illustrates that WiCyS members outperformed others in most of the specialty areas within the NICE Framework. This is especially notable in domains such as:

***Executive Cyber Leadership** +11*
***Cyber Defense Analysis** +7*
***Cyber Defense Infrastructure Support** +7*
***Systems Administration** +7*
***Legal Advice and Advocacy** +6*
***Cyber Operational Planning** +6*
***Risk Management** +7*
***Strategic Planning and Policy** +4*
***Vulnerability Assessment and Management** +3*
***Cybersecurity Management** +2*

WiCyS members scored higher in these NICE specialty areas than other participants, underscoring their advanced capabilities and deep understanding of complex cybersecurity disciplines.

These strengths suggest that WiCyS's programs and initiatives are particularly effective in these domains, providing members with a strong foundation to excel in strategic and operationally critical areas of cybersecurity.

OPPORTUNITIES FOR DEVELOPMENT

While the overall performance of WiCyS members is commendable, the chart also highlights specific areas where their scores were slightly lower than those of other participants who have taken the same diagnostic. These Specialty Areas include:

***Software Development** –3*
***Incident Response** –2*
***Systems Analysis** –2*

The performance gap in these fields suggests potential opportunities for WiCyS to enhance its programs. Focusing on these areas could help address existing skill gaps and ensure members are equally prepared in all aspects of cybersecurity.

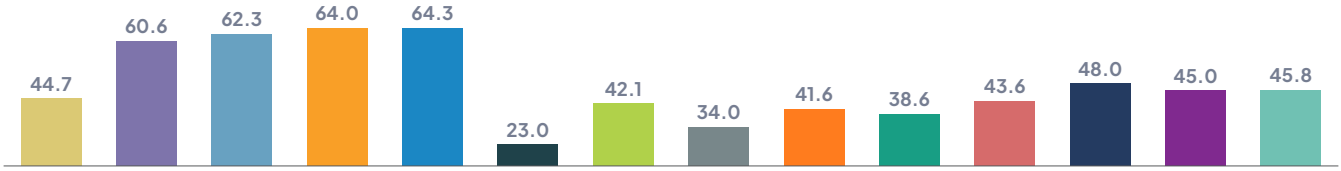
These results have profound implications. They underscore the effectiveness of WiCyS's programs in preparing its members for significant roles within the cybersecurity industry and highlight the potential for these members to lead and innovate across the industry. The data clearly demonstrates the value of investing in WiCyS, showcasing the organization's leadership in promoting diversity and excellence in cybersecurity.

WiCyS MEMBER EXCELLENCE IN N2K FUNCTIONAL GROUPS

This section of the report explores the accomplishments and insights from the in-depth skills analysis carried through the lens of N2K's Functional Groups & Taxonomy. All scoring metrics presented in this section are an insular examination of the WiCyS member participants as a group, rather than a comparison to other scores from non-WiCyS Talent Study participants. By analyzing performance data in this way, N2K is able to identify areas of strength and areas of opportunities for participants based on the Functional Group they associate with as a part of their profession.

WiCyS Participants Composition by N2K Functional Groupings:

Summary of Participant RPS Scoring by N2K Functional Group:



Relative Performance Score (RPS): an N2K scoring metric that excludes questions that are not relevant to Work Roles or Specialty Areas that align to each N2K Functional Group, and instead only measures performance on questions that are most-relative to the typical knowledge and competencies expectations for each Functional Group or Work Role.

In addition to the NICE Framework Specialty Areas, N2K has classified the NICE Specialty Areas into broader Functional Groups as part of the methodology for this report. WiCyS members have demonstrated superior performance across four major functional groups:

Communications & Network Security

Members excel in this area, demonstrating their ability to effectively manage and secure complex network infrastructures.

Cybersecurity WF & Awareness

This area highlights WiCyS members' capacity to effectively educate and raise awareness within the industry. The performance data suggests a strong foundation in training and mentorship, which is critical for the ongoing development of the cybersecurity workforce.

Cybersecurity/IT Leadership & MGMT

WiCyS members demonstrate strong leadership capabilities essential for advancing within the cybersecurity industry.

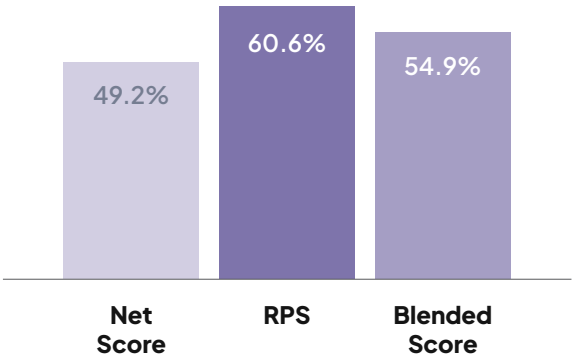
Cybersecurity/IT Policy & GRC

Members demonstrate a sophisticated grasp of governance, risk, and compliance issues critical to organizational cybersecurity strategies.

COMMUNICATIONS & NETWORK SECURITY - CNS

The Communications and Network Security functional area is critical in safeguarding an organization's digital communications and infrastructure. This domain demands a deep understanding of network protocols such as IPSec, IPv4, IPv6, and both secure and converged protocols, as well as wireless and cellular networks. Professionals in this field are tasked with designing, implementing, and maintaining secure communication channels that protect against unauthorized access and threats and ensure data confidentiality, integrity, and availability.

Scoring of WiCyS Members by This Functional Group:



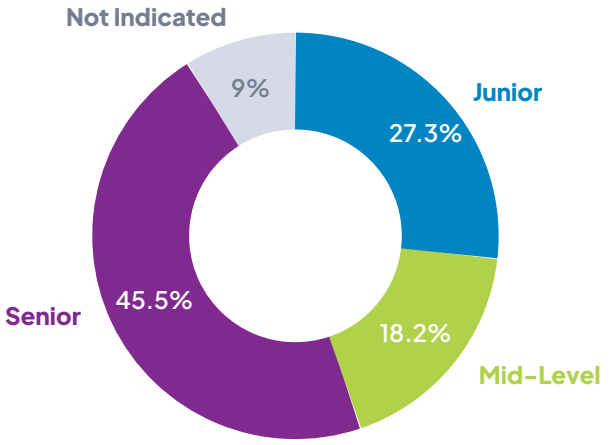
Net Score: measures performance across all questions provided despite any Work Role or Functional Group knowledge/ competency expectations.

Relative Performance Score (RPS): an N2K scoring metric that excludes questions that are not relevant to Work Roles or Specialty Areas that align to each N2K Functional Group, and instead only measures performance on questions that are most-relative to the typical knowledge and competencies expectations for each Functional Group or Work Role.

Blended Score: the average of Net Score and RPS values.

WiCyS members have shown remarkable proficiency in Communications and Network Security, outperforming their peers in mastering these complex systems. Their skills are not limited to identifying potential vulnerabilities and implementing security measures; they also excel in troubleshooting and resolving intricate network issues. This superior performance indicates their comprehensive training and ability to overcome emerging security challenges. Moreover, WiCyS members' capabilities extend to effective collaboration with third-party vendors and partners, ensuring secure connectivity and rigorous adherence to security policies and standards. This level of expertise underscores the exceptional capability of WiCyS members to lead and innovate within this essential cybersecurity domain, reflecting their critical role in advancing industry standards and enhancing organizational security posture.

Exp. Levels of WiCyS Members by This Functional Group:



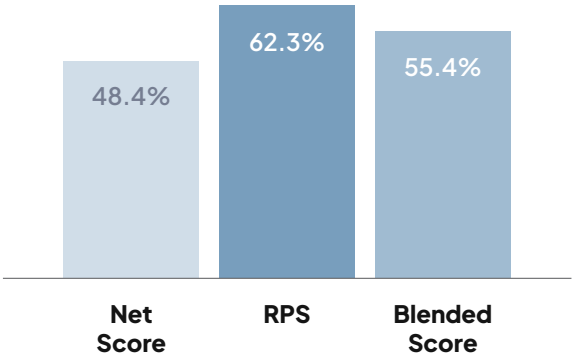
Functional Group Definition:

This functional area involves designing, implementing, and maintaining secure communication channels and networks within an organization. Tasks may include assessing existing communication and network infrastructure to identify potential vulnerabilities and implementing security measures to mitigate risks to ensure confidentiality, integrity, and availability of data. The functional area requires in-depth knowledge of network protocols such as IPSec, IPv4, IPv6, secure and converged protocols, and wireless and cellular networks. Responsibilities include the ability to troubleshoot and resolve technical communications and networking issues, including liaising with third-party vendors and partners to establish secure connectivity and ensure compliance with security policies and standards.

CYBERSECURITY WORKFORCE TRAINING & AWARENESS - WTA

The Cyber Workforce, Training, & Awareness functional area is pivotal in strengthening an organization's cybersecurity posture by developing a knowledgeable and skilled workforce. This crucial domain ensures the organization has qualified personnel with the necessary skills and knowledge to meet its cybersecurity demands. Responsibilities include identifying essential skills and career pathways for cybersecurity roles, developing comprehensive training programs, and delivering regular training sessions to keep employees abreast of evolving threats and best practices.

Scoring of WiCyS Members by This Functional Group:



Net Score: measures performance across all questions provided despite any Work Role or Functional Group knowledge/ competency expectations.

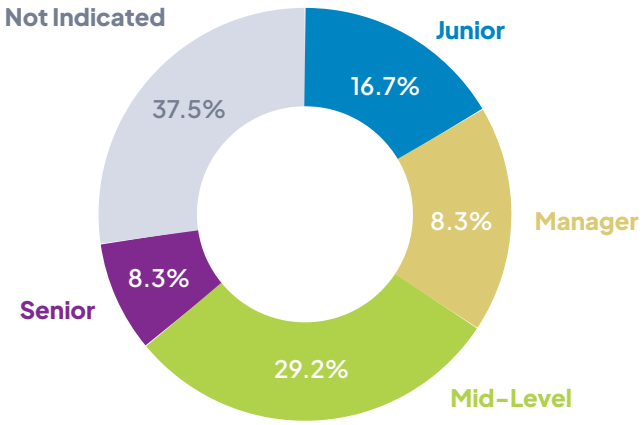
Relative Performance Score (RPS): an N2K scoring metric that excludes questions that are not relevant to Work Roles or Specialty Areas that align to each N2K Functional Group, and instead only measures performance on questions that are most-relative to the typical knowledge and competencies expectations for each Functional Group or Work Role.

Blended Score: the average of Net Score and RPS values.

WiCyS members have demonstrated exceptional strength in developing and implementing effective training strategies. Their expertise covers creating and delivering targeted training programs and extends to assessing their effectiveness. WiCyS members excel in measuring employee understanding and adherence to cybersecurity policies and procedures, ensuring that training outcomes align closely with organizational security goals.

Furthermore, WiCyS members are adept at overseeing the procurement and implementation of training resources, ensuring that both technical teams and general staff are well-equipped to counteract current and emerging cyber threats. This comprehensive approach to cybersecurity training and awareness highlights the proactive and strategic role WiCyS members play in enhancing the security culture within organizations, making them invaluable cybersecurity education and workforce readiness leaders.

Exp. Levels of WiCyS Members by This Functional Group:



Functional Group Definition:

This functional area ensures the organization's cyber security posture by building a cyber-savvy workforce and ensuring the organization has enough qualified personnel with the necessary skills and knowledge to meet its cyber security needs. This includes identifying the skills, knowledge, and career pathways required for various cyber security roles within the organization, developing and delivering training programs, and conducting regular cyber security training sessions to keep employees up-to-date with evolving threats and best practices. The functional area also oversees the procurement and delivery of training implementations for the cyber workforce as well as security awareness training for the enterprise. This would also include assessing the effectiveness of cyber security training and awareness programs by measuring employee knowledge and understanding of cyber security policies and procedures.

CYBERSECURITY/IT LEADERSHIP & MANAGEMENT - LSP

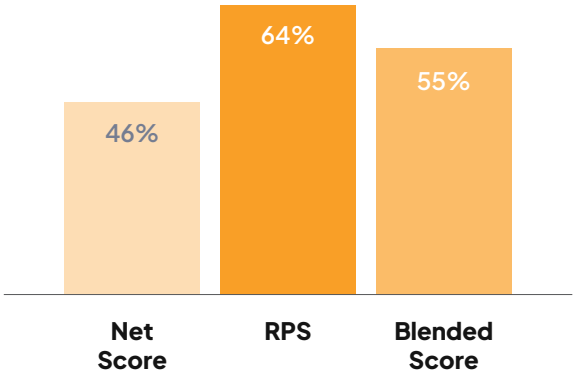
The Cyber/IT Leadership & Management functional area is critical for steering an organization's cybersecurity and IT strategy toward success. This domain encompasses the knowledge and skills necessary for executive decision-making, vision setting, and directing an organization's IT and cybersecurity resources and operations. Leaders in this area oversee various activities that span risk management, budgeting, workforce decisions, and vendor management, all viewed through a leadership and management lens.

WiCyS members have showcased superior proficiency in Cyber/IT Leadership and Management, highlighting their ability to effectively guide cybersecurity initiatives. In addition to their technical skills, members demonstrate a strategic acumen that aligns cybersecurity strategies with broader business objectives. These leaders excel in integrating concepts related to business strategy, processes, and technology within team and organizational contexts, ensuring that cybersecurity measures support overall corporate goals.

Additionally, WiCyS members in this role demonstrate exceptional skills in managing budgets and resources, making strategic workforce decisions, and handling vendor relationships, which are crucial for maintaining robust cybersecurity frameworks. Their leadership extends beyond management; they inspire and cultivate a culture of security awareness and compliance throughout their organizations.

This distinctive blend of technical knowledge and strategic leadership empowers WiCyS members to drive significant improvements in their organizations' cybersecurity postures, positioning them as indispensable leaders in the ever-evolving cyber/IT landscape. Their comprehensive approach ensures that cybersecurity is about protecting assets and enabling and supporting business growth and innovation.

Scoring of WiCyS Members by This Functional Group:

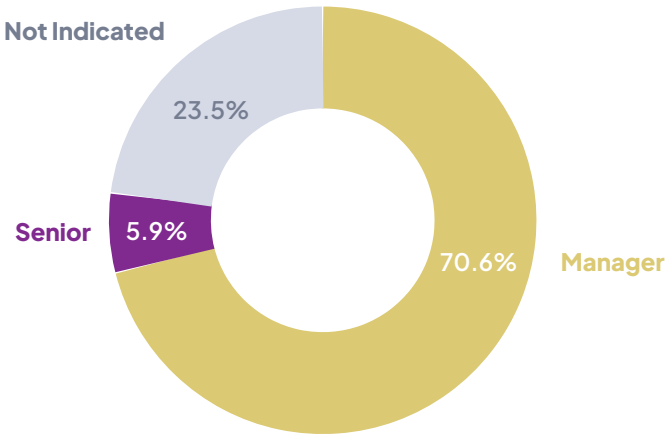


Net Score: measures performance across all questions provided despite any Work Role or Functional Group knowledge/ competency expectations.

Relative Performance Score (RPS): an N2K scoring metric that excludes questions that are not relevant to Work Roles or Specialty Areas that align to each N2K Functional Group, and instead only measures performance on questions that are most-relative to the typical knowledge and competencies expectations for each Functional Group or Work Role.

Blended Score: the average of Net Score and RPS values.

Exp. Levels of WiCyS Members by This Functional Group:



Functional Group Definition:

This functional group covers knowledge and skills that enable executive decision-making authority and establishes vision and direction for an organization's cyber/IT and related resources and/or operations. The topics under this functional area may span the same or similar topics included with other functional areas but with a leadership/ management lens or perspective (including risk management, budgeting, workforce decisions, and vendor management). Emphasis is placed on concepts that relate back to business strategy, processes, and technology with a team or broader organizational context.

CYBERSECURITY/IT POLICY & GOVERNANCE, RISK, & COMPLIANCE - GRC

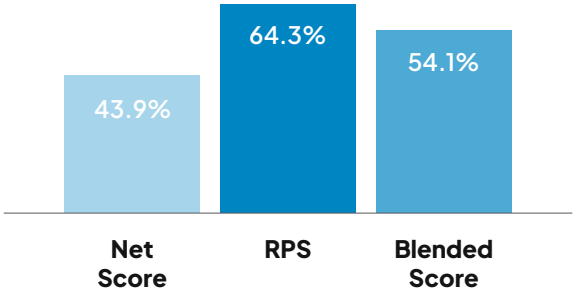
The Cyber/IT Policy & Governance, Risk, and Compliance functional area ensures that an organization's cybersecurity and IT operations are tightly aligned with established governance structures and regulatory requirements. This critical domain focuses on articulating clear governance frameworks that delineate roles and responsibilities while integrating IT and cybersecurity risks into the broader risk management strategy of the organization. Professionals in this field are tasked with developing, maintaining, and enforcing robust cyber and IT policies, procedures, and standards that resonate with the organization's strategic objectives.

WiCyS members have demonstrated exemplary performance in this area, excelling in their capacity to ensure organizational compliance with a range of international and domestic regulations, such as PCI-DSS, GDPR, and HIPAA. Their expertise is not limited to compliance alone; they also excel in effectively communicating and training employees on IT policies and procedures, cultivating a cybersecurity awareness culture throughout the organization.

Furthermore, WiCyS members are proficient in conducting thorough risk assessments that evaluate potential vulnerabilities and align cybersecurity strategies with business needs. This proactive approach mitigates risks and enhances the organization's resilience against cyber threats.

The ability of WiCyS members to stay abreast of the latest regulations and to adapt governance frameworks accordingly positions them as critical assets in their organizations. They play a pivotal role in ensuring that cybersecurity measures are not just reactive but are proactive and integrated elements of the broader business strategy. This strategic integration ensures that organizations comply with necessary regulations and leverage their cybersecurity practices as a competitive advantage in their respective industries.

Scoring of WiCyS Members by This Functional Group:

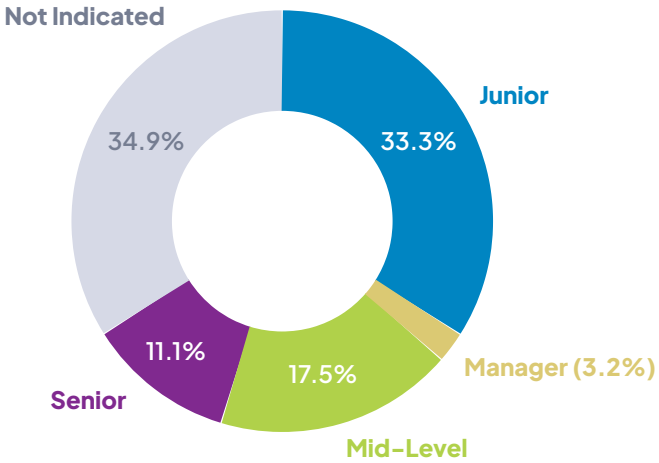


Net Score: measures performance across all questions provided despite any Work Role or Functional Group knowledge/competency expectations.

Relative Performance Score (RPS): an N2K scoring metric that excludes questions that are not relevant to Work Roles or Specialty Areas that align to each N2K Functional Group, and instead only measures performance on questions that are most-relative to the typical knowledge and competencies expectations for each Functional Group or Work Role.

Blended Score: the average of Net Score and RPS values.

Exp. Levels of WiCyS Members by This Functional Group:



Functional Group Definition:

This functional area focuses on defining the governance structure for managing cyber and IT risks—including roles and responsibilities—and ensuring that cyber and IT risks are integrated into the organization's overall risk management framework. Other areas of focus include developing, maintaining, and enforcing cyber and IT policies, procedures, and standards considering the organization's overall strategy and objectives; and communicating and training employees on such IT policies and procedures. Professionals in this functional area need to stay up-to-date with relevant regulations, laws, and standards (i.e., PCI-DSS, GDPR, HIPAA, etc.) and ensure the organization stays in compliance with any applicable requirements. Overseeing and/or conducting periodic risk assessments also fall within the scope of this functional area.

“The N2K Cyber Talent Study highlighted areas in security where I need improvement. This insight has helped my study efforts for the CISSP exam and helped me identify specific skills to enhance my career advancement. I anticipated weaknesses in the technical aspects of security, the assessment confirmed and clarified these gaps. Understanding technical concepts is important to me, even though my role is not technically focused. This broader knowledge base strengthens my overall competence in the field.”

Nicole Ogertschnig
Manager of Risk Management,
American Express

WiCyS STRATEGIC INITIATIVES

The results of the N2K and WiCyS collaboration highlight the current strengths and capabilities of WiCyS members and frame the strategic direction for future initiatives. These insights are invaluable in shaping programs that are proactive in addressing the evolving needs of the cybersecurity landscape.

As WiCyS continues to lead in the recruitment, retention, and advancement of women in cybersecurity, the data from this study provides a strong foundation for targeted program development. The initiatives poised for implementation include:

Skills Development Training Programs:

Building on their expansive professional development training programs, WiCyS uses detailed performance data to enhance and expand training modules. This strategic approach reinforces existing strengths and ensures members continue evolving and aligning with the latest industry demands.

Mentorship Expansion:

Building on the success of existing mentorship programs, WiCyS intends to broaden these opportunities, connecting more experienced professionals with newcomers to foster a supportive and knowledgeable community.

Security Training Scholarships:

Powered by partnerships with top-tier supporters, the WiCyS Security Training Scholarship exemplifies strategic ingenuity in developing the cybersecurity talent pipeline. This multi-staged scholarship is designed specifically for WiCyS members poised to enter the cybersecurity workforce within the next 1.5 years, including students and career changers seeking to pivot into the cybersecurity industry.

These strategic initiatives are designed to leverage the strengths identified in the study and ensure that WiCyS members are well-equipped to meet and exceed the cybersecurity industry's demands.

OPPORTUNITIES FOR GROWTH AND PARTNERSHIP

The collaboration between N2K and WiCyS also highlights several key areas for growth and partnership, offering potential sponsors and partners the opportunity to make a significant impact. The analysis identified specific areas such as Systems Analysis, Software Development, and Incident Response fields where strategic development could yield substantial advancements.

Highlighting Potential

The data shows WiCyS members possess potential across some cybersecurity domains. By focusing on strategic areas for development, WiCyS can further enhance its members' skills and readiness for advanced roles.

Role of Corporate Sponsorhip

Corporate sponsors have a significant opportunity to contribute to the growth of these areas. Sponsors can help WiCyS members succeed by supporting specialized training programs, mentorship programs, and professional development resources.

Mutual Benefits

The benefits of such partnerships extend beyond the direct impact on WiCyS members. Sponsors gain access to a pool of top-tier talent and the opportunity to be recognized as leaders in promoting diversity and excellence in cybersecurity.

This cooperative effort drives the professional growth of individual members and contributes to the broader goal of creating a diverse, capable, and resilient cybersecurity workforce.

"It has been an enriching experience that has not only provided me with valuable insights into cybersecurity but also equipped me with **the necessary tools to further my knowledge in this critical field.**"

Lucy Chambliss
Cybersecurity Analyst

CLOSING INSIGHTS: WiCyS'S COMMITMENT TO DIVERSITY AND INDUSTRY LEADERSHIP

This report reflects the current state of WiCyS member participation and performance in cybersecurity as facilitated by N2K. It charts a path forward for enhancing this involvement through strategic initiatives and partnerships. The collaboration between N2K and WiCyS has been instrumental in highlighting the critical role that a diverse and well-equipped workforce plays in advancing the field of cybersecurity.

The insights derived from this study are a testament to the power of collaborative efforts to drive significant advancements in industry-wide practices and individual career trajectories. We encourage all stakeholders in the cybersecurity ecosystem—corporate sponsors, educational institutions, policymakers, and industry leaders—to engage with and support WiCyS's mission. Together, we can build a diverse, robust cybersecurity workforce that can address the complex challenges of today and tomorrow.

Your support and involvement can make a pivotal difference in turning these insights into actions that promote diversity in cybersecurity and enhance the overall efficacy and innovation within the field.

ADDITIONAL RESOURCES

- **WiCyS State of Inclusion Assessment:** www.wicys.org/initiatives/wicys-state-of-inclusion/
- **N2K's Cyber Talent Insights:** www.n2k.com/talent-insights
- **N2K and WiCyS interview on N2K CyberWire:** www.thecyberwire.com/podcasts/special-edition/66/notes

WiCyS CONTRIBUTORS:

Lynn Dohm
Executive Director,
WiCyS

Mary Jane Suarez Partain
Program Director,
WiCyS

N2K AUTHORS:

Simone Petrella
President,
N2K

Jeff Welgan
Chief Learning Officer,
N2K

Heather Monthie, PhD, CISSP
Workforce Consultant,
N2K

Interested in benchmarking your organization's workforce capabilities and job roles to maximize your talent investments, contact us at talentinsights@n2k.com.

About N2K

N2K Networks is a leader in strategic cyber workforce intelligence. The news to knowledge network is a trusted source of Industry Insights delivered through our media network, home of the CyberWire Daily podcast and daily briefing, CSO Perspectives, and Hacking Humans, which provides concise intelligence-driven news and commentary to cybersecurity professionals. Global enterprise organizations, including those in the Fortune 100, partner with N2K to gain actionable cyber workforce insights through our Talent Insights and Talent Development capabilities that help organizations build and maintain high-performing teams, rapidly climb the knowledge curve, and stay a step ahead in a constantly changing industry. Learn more at **N2K.com**.

About WiCyS

Women in CyberSecurity (WiCyS) is a nonprofit organization with international reach dedicated to the recruitment, retention and advancement of women in cybersecurity. Founded by Dr. Ambareen Siraj through a National Science Foundation grant given to Tennessee Tech University in 2013, WiCyS offers opportunities, trainings, events, and resources for its community and members. Strategic partners include Tier 1: Akamai Technologies, Amazon, Bloomberg, Carnegie Mellon University Software Engineering Institute, Cisco, Ford Motor Company, Google, LevelBlue, Lockheed Martin, Microsoft, Optum, Sandia National Laboratories, SentinelOne. Tier 2: Accenture, Adobe, DeVry University, Intel, JPMorgan Chase & Co., McKesson Corporation, MITRE, Motorola Solutions, Navy Federal Credit Union, Workday. To partner, visit **www.wicys.org/support/strategic-partnerships/**.

N2K Networks
8110 Maple Lawn Blvd, Ste 200
Fulton, MD 20759