ACM Joint Task Force to Develop Global Cybersecurity Curricular Guidelines
Survey Report – November 2016

INTRODUCTION

The ACM Joint Task Force on Cybersecurity Education (JTF) launched in September 2015 to develop the first set of global curricular guidelines in cybersecurity education. Cybersecurity is defined here as:

> *"A computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries."*

The JTF is a collaboration between major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). The JTF grew out of the foundational efforts of the Cyber Education Project (CEP).

After a year of community engagement and developmental work, the JTF launched a survey in September 2016 to solicit broad input on the proposed curricular thought model. Stakeholders were invited to participate in the survey through direct invitations, announcements in public educational and scientific forums, social media outreach via the JTF website and LinkedIn, and invitations sent through the distribution lists of participating professional associations. This report summarizes the 231 completed survey responses received during the survey period of September 16 – October 3, 2016.

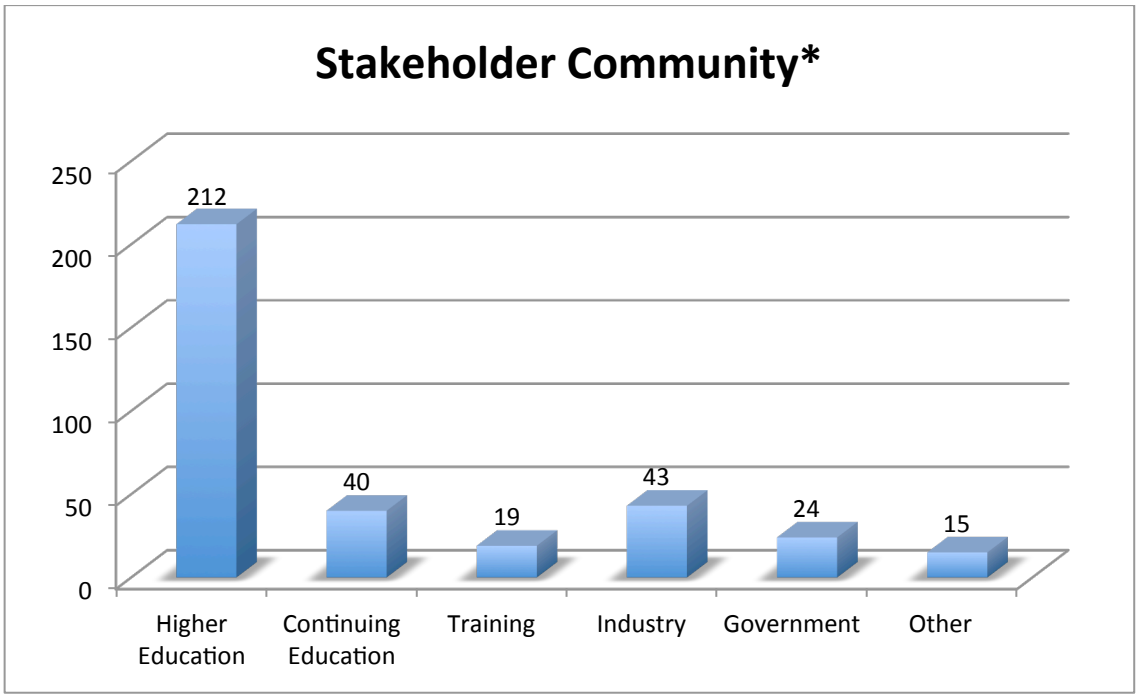
RESPONDENT DEMOGRAPHICS

Gender: Approximately 71% (163) of respondents were male, 26% (60) were female, and eight respondents did not indicate gender.

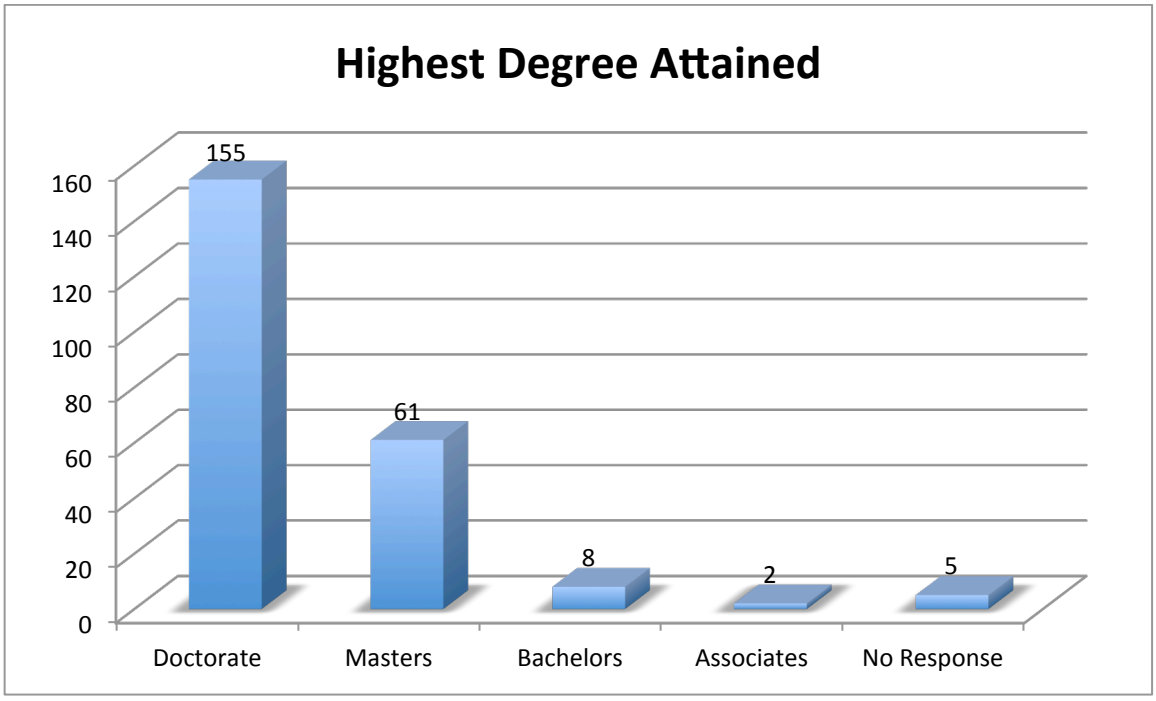
Geographic distribution: Nearly 88% (201) of survey respondents reported the United States as their primary work location. The remaining 22% of survey respondents were distributed as follows[1]: Australia (5), Norway (3), Italy (2), South Africa (2), and Sweden (2) Canada (2), China (2); with one completed survey from each of the following countries: Bulgaria, Hong Kong, India, Netherlands, New Zealand, Portugal, Qatar, Singapore, Slovenia, South Korea, Spain, and Thailand.

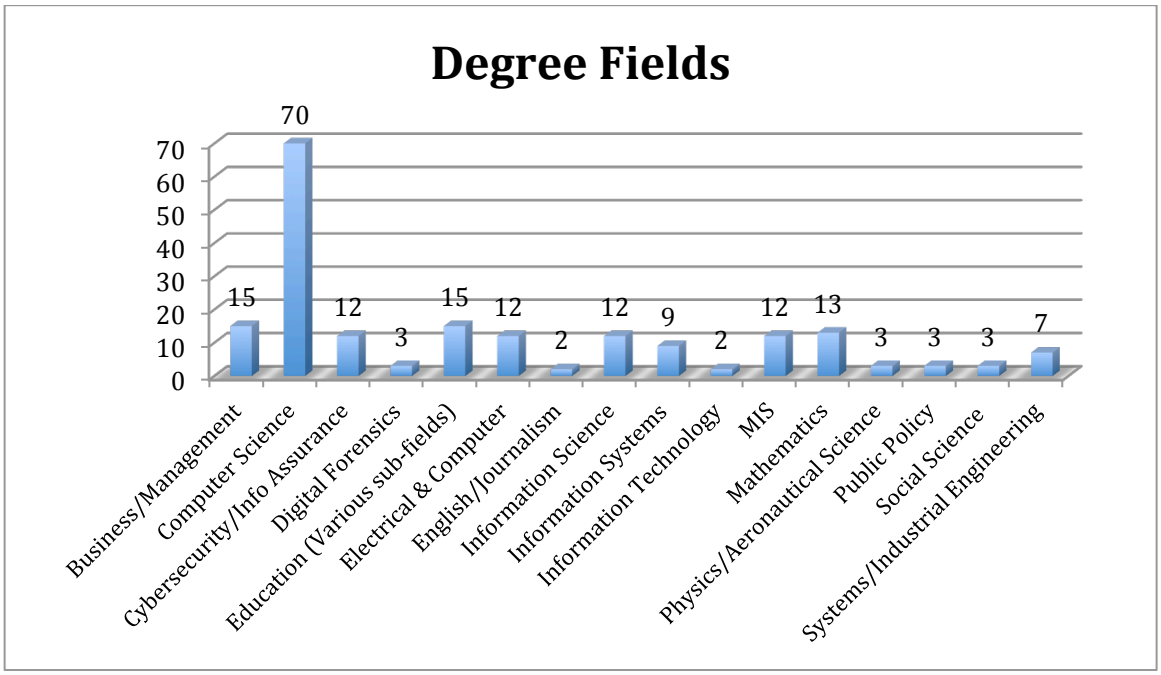
[1] The number of respondents per country is shown in the parentheses.

The charts below provide additional information on the background of survey respondents.

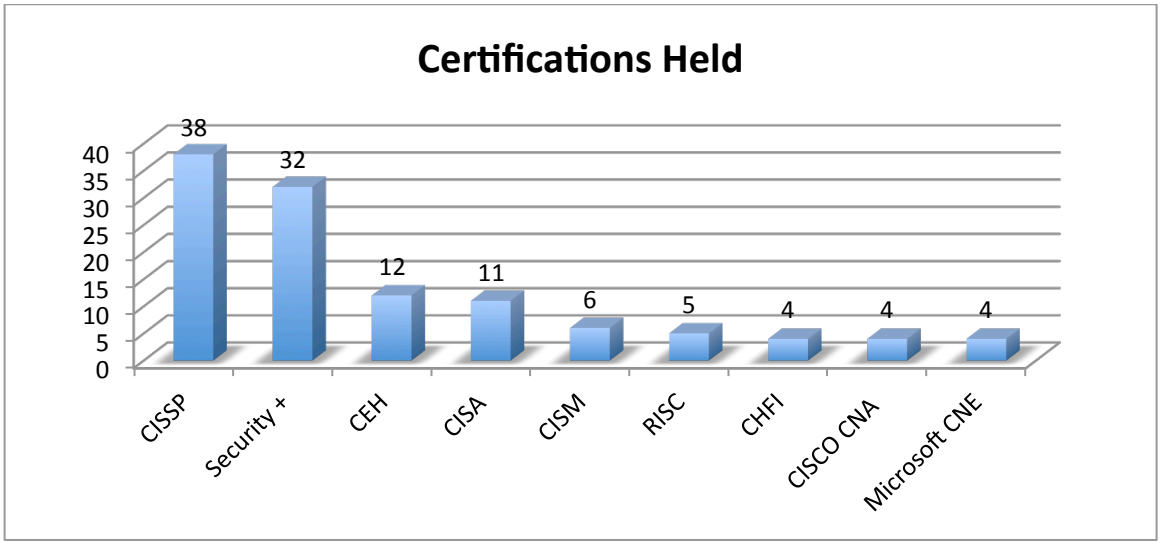


*Respondents were permitted to select all applicable stakeholder groups.





^Degree fields represent all degree levels (doctorate, masters, bachelors, and associates).



Many respondents reported holding multiple certifications. The most frequently held certifications included: the Certified Information Systems Security Professional (CISSP), Security +, Certified Ethical Hacker (CEH), Certified Information Auditor (CISA), Certified Information Security Manager (CISM), Risk and Information System Control (RISC), Computer Hacking Forensic Investigator, Cisco Certified Network Associate, and

Microsoft Certified Systems Engineer. Certifications held by three or fewer respondents included Certified Cyber Forensics Professional, Project Management Professional, Cisco Certified Network Associate (Security), or Certified Could Security Professional. Of the 231 respondents, 33 reported that they did not hold a security-related certification.

FEEDBACK ON THE PROPOSED THOUGHT MODEL

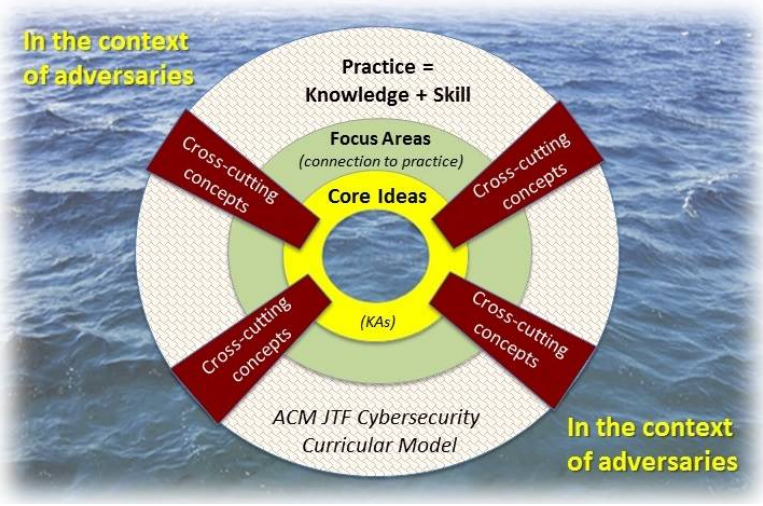
Survey participants were asked to provide feedback on the JTF curricular thought model. The curricular thought model was presented as a modification of U.S. National Research Council Next Generation Science Standards (nextgenscience.org). Survey respondents were asked to comment specifically on (1) the graphical representation and (2) the four structural elements of the thought model: Core Ideas, Focus Areas, Practices, and Cross-Cutting Concepts for cybersecurity education.

- **Core Ideas** are knowledge areas or domains;
- **Focus Areas** are different professional practice contexts;
- **Practices** are the combination of knowledge and skills that culminate into competency when connected with a particular focus area; and
- **Cross-Cutting Concepts** bridge core ideas practice and focus areas.

Feedback on each component is provided below.

(1) Graphical Representation

Survey respondents were asked to consider the proposed graphic and respond to the 3 questions listed in the table below.



	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1 - The above graphic clearly communicates that engaging in cybersecurity investigation requires not only skill but also knowledge that is specific to each Practice	**48** (20.8%)	**81** (35.1%	**32** (13.9%)	**53** (22.9%)	**17** (7.4%)
Q2--The above graphic clearly communicates that Cross-Cutting Concepts bridge Core Ideas, Practices, and Focus Areas.	**73** (31.6%)	**92** (39.8%	**23** (10.0%)	**33** (14.3%)	**10** (4.3%)
Q3 --The above graphic clearly communicates that Core Ideas have the power to focus cybersecurity curriculum, instruction and assessments.	**32** (13.9%)	**68** (29.4%	**53** (22.9%)	**55** (23.8%)	**23** (10.0%)

As indicated by the responses to each question, survey respondents were generally favorable about the graphic. However, a summary of the 73 comments offered as respondent narratives, suggest several areas for improvement:

- Include specific Practice Areas and revise the graphic to show that multiple practice areas exist.
- Expand the definition of each of the model elements and clarify the distinction between them.
- Align the graphical representation and the model more tightly. The current representation is not intuitive or easily understood without the model.
- Simplify the diagram.

(2) Structural Elements of the Thought Model

Summary feedback on each the four structural elements of the thought model: Core Ideas, Focus Areas, Practices, and Cross-Cutting Concepts for cybersecurity education; is provided below.

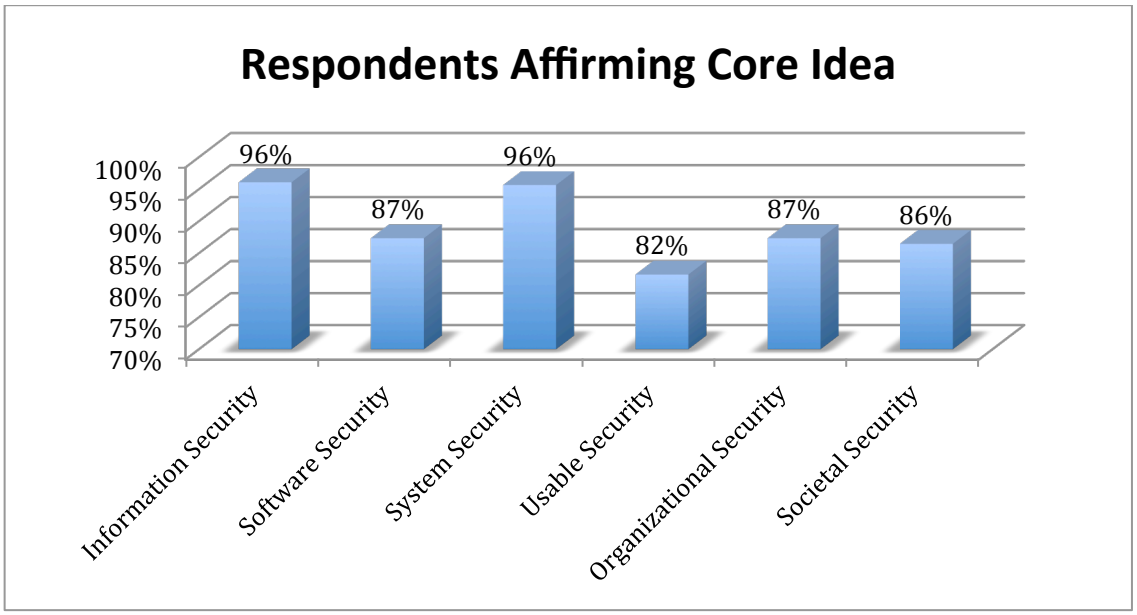
Core Ideas

Core Ideas are defined as knowledge areas or domains. Survey respondents were asked to review the Core Ideas listed below and (A) indicate if each listed Core Idea should be included in the curricular volume; (B) suggest any changes to the definition of the Core Idea and recommend the addition of Core Ideas not currently included.

Core Ideas:

1. Information Security [Includes: information confidentiality, data integrity, availability, cryptography and cryptanalysis]
2. Software Security [Includes: secure software engineering, software reverse engineering, malware analysis]
3. System Security [Includes: availability, authentication, access controls, secure systems design, computer network defense and CNA/penetration testing, reverse engineering (hardware), cyber physical systems, digital forensics, supply chain mgmt.]
4. Usable Security [Includes: identity management, social engineering, social networks, human-computer interaction]
5. Organizational Security [Includes: risk management, mission assurance, disaster recovery, business continuity, security evaluations/compliance, organizational behavior, intelligence, economics]
6. Societal Security [Includes: cyber crime, cyber law, ethics, policy, privacy, intellectual property, professional responsibility, global societal impacts]

(A) Percentage of respondents affirming Core Idea



(B) Summary Comments on the Core Ideas

Survey respondents made several recommendations regarding the list of Core Ideas. The recommendations summarized below reflect the themes for each Core Idea.

Information Security

- Reconsider the inclusion of cryptography and cryptanalysis. These topics should be removed as Core Ideas and instead included as topics for specific groups.
- Provide a more thorough rationale for the set of Core Ideas included in the model. As they are presented, the breadth of topics does not provide sufficient curricular focus.
- Include topics of privacy authentication and non-repudiation. If these topics are addressed in the existing categories, clarify their placement.

Software Security

- Many of the topics included in the category are specialized and might not be relevant for the all portions of the broad audience to be served by this document. Given this, should the topics here be re-classified.
- Reconsider the inclusion of topics that seem more related to practice. For example, malware analysis and reverse engineering might be more appropriately classified as a practice rather than a core idea.
- Provide a stronger reference to, and consider relabeling this category as, the security software development lifecycle.

System Security

- Several topics, while important for some specialized areas, are not relevant for the broad audience to be served by this document. For instance, CNA, digital forensics, and supply chain management should not be listed as Core Ideas.
- Reconsider the inclusion of topics that seem more related to practice. For example, hardware reverse engineering should be removed.

Usable Security

- Identity management is a critical topic related to access control but is misplaced in this category. Move it to Organizational Security.
- Consider relabeling this category. Is the theme here 'user' or 'human factors' security? If so, consider using one of these labels to clarify the meaning of 'usable' security.
- Many of the ideas included in this category are tightly coupled with practice. This content may be misclassified as a Core Idea.

Organizational Security

- The topics included in this category are important but reconsider whether or not they have the same level of importance as the other categories.
- Risk management is a critical topic but the other content included in this category may not be as important. For example, is economics important to include here.
- Critical, but missing, topics include resilience and physical security. These topics should be added.

Societal Security

- The topics included in this category are important but reconsider whether or not they have the same level of importance as the other categories. Privacy is the only exception to this comment.
- The category is extremely broad. Identify the specific topics to be included here.

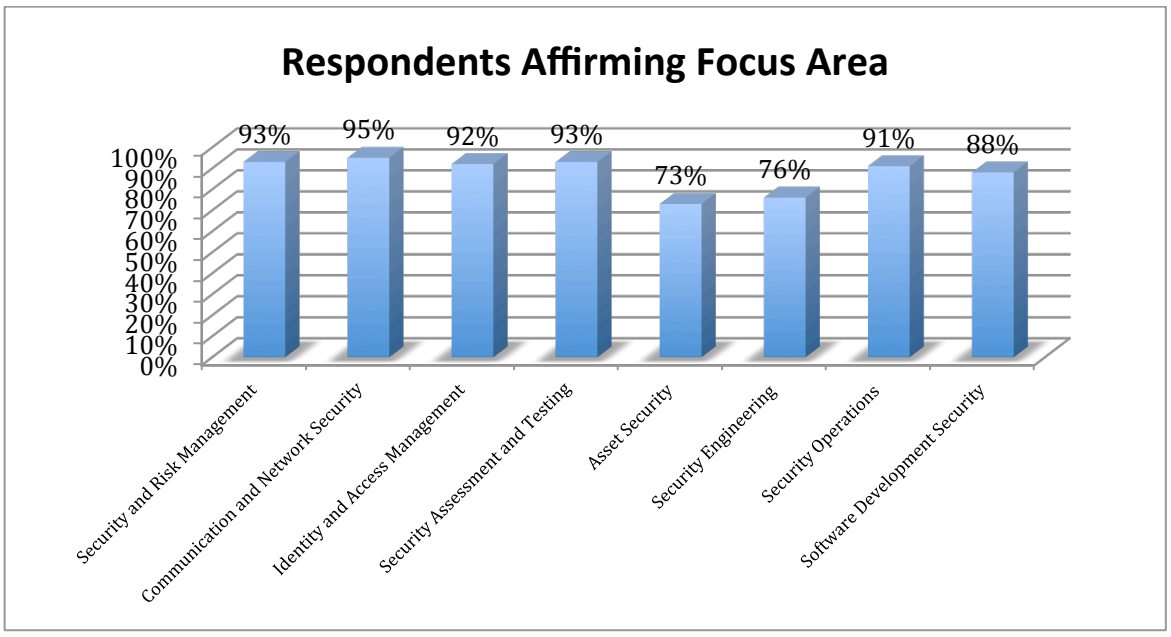
Focus Areas

Focus Areas are defined as different professional practice contexts. Survey respondents were asked to review the Focus Areas listed below and (A) indicate if each listed Focus Area should be included in the curricular volume; (B) suggest any changes to the definition of the Focus Area and recommend the addition of Focus Areas not currently included.

Focus Areas:

1. Security and Risk Management [Includes: Security, Risk, Compliance, Law, Regulations, and Business Continuity]
2. Communication and Network Security [Includes: Designing and Protecting Network Security]
3. Identity and Access Management [Includes: Controlling Access and Managing Identity]
4. Security Assessment and Testing [Includes: Designing, Performing, and Analyzing Security Testing]
5. Asset Security [Includes: Protecting Security of Assets]
6. Security Engineering [Includes: Engineering and Management of Security]
7. Security Operations [Includes: Foundational Concepts, Investigations, Incident Management, and Disaster Recovery]
8. Software Development Security [Includes: Understanding, Applying, and Enforcing Software Security]

(A) Percentage of respondents affirming Focus Area



(B) Summary Comments on the Focus Areas

Survey respondents made several recommendations regarding the list of Focus Areas. The recommendations summarized below reflect the themes for each Focus Area.

Security and Risk Management

- Change the label of this category to "Governance, Risk, and Compliance" in order to highlight the importance of each of these topics.
- Reconsider the inclusion of business continuity. While it is an important topic, is it appropriately categorized here?
- Add audit to this category.

Communication and Network Security

- The content of this Focus Area should be reclassified as a Core Idea.
- Clarify the definition of the category and more precisely describe the content.

Identity and Access Management

- The content of this Focus Area is important, but may be too narrowly defined to stand as a separate category.

Security Assessment and Testing

- This category should include certification and audit.
- While important topics, this category is too narrow and should be combined with another focus area.

Asset Security

- Clarify the definition of assets (e.g. digital/physical/information) in this category.
- While important topics, this category is too narrow and should be combined with another focus area.

Security Engineering

- Clarify the definition of security engineering as a focus area.
- Exclude management from this category.

Security Operations

- Clarify the foundation concepts to be included in this category.
- Respondents affirmed the importance of this content within this category but were conflicted about whether the category was too broadly or too narrowly defined.

Software Development Security

- Clarify how this category differs from security engineering and from security operations. Should the categories be combined?

Other Comments

- Additional topics to include: incident management, ethics, social engineering, physical security, and policy.
- How were these areas determined? Consider using the NIST Framework and leveraging the categories: Identify, Protect, Detect, Respond, and Recover.
- Several overlapping areas of management should be included.

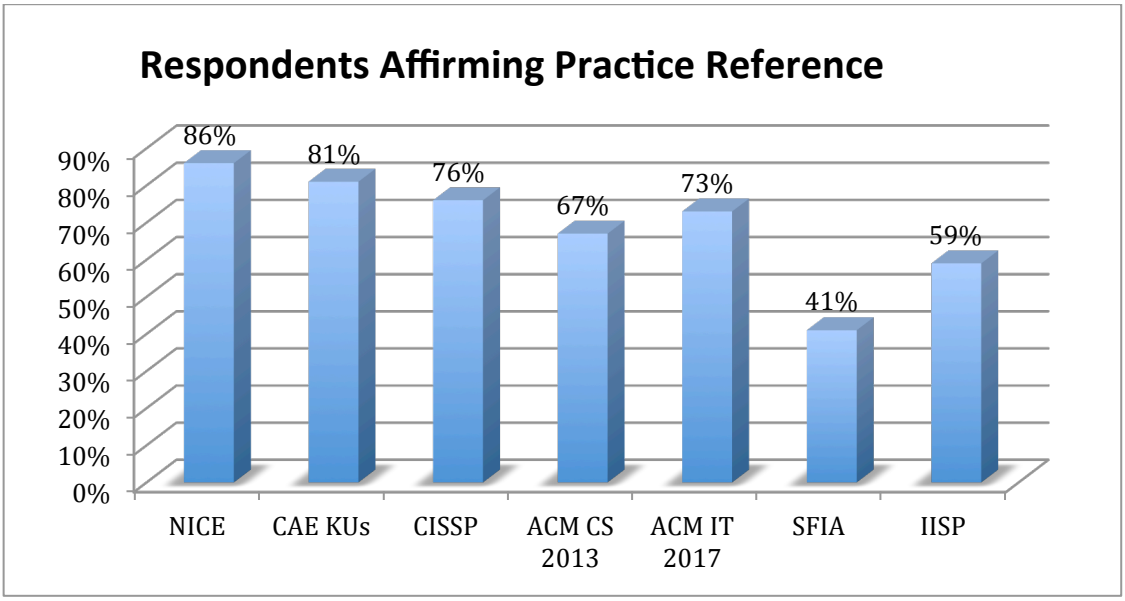
Practice

Practices are the combination of knowledge and skills that culminate into professional competency when connected with a particular Focus Area. Survey respondents were asked to consider the list of references below and (A) indicate if the practices derived from those sources should be included in the cybersecurity curricular volume; and (B) suggest any additional sources to include.

Practice:

- National Cybersecurity Workforce framework – NICE
- NSA Center of Academic Excellence, Knowledge Units - NSA KU
- (ISC)2 Certified Information Systems Security Professional – CISSP
- ACM Computer Science Curricula 2013 - CS 2013
- ACM/IEEE Information Technology Curriculum 2017 - IT 2017
- Skills Framework for the Information Age – SFIA
- Institute for Information Security Professionals Framework 2.0 - IISP 2.0

(A) Percentage of respondents affirming Practice Reference



(B) Summary Comments on Practice References

- Do not lean to heavily on any of these references. The relative quality and value of various references was mixed and many respondents noted that relevance will depend on the audience.
- The references are heavily US-centric. Add additional global reference points.
- Articulate how the inclusion of these practice references aligns with the purpose of the curricular volume. The references have many overlapping concepts and the inclusion of multiple frameworks will be confusing. A significant contribution of this volume would be to provide a guide to overlapping practices in these, and other frameworks.
- Cautiously distinguish between education and training – developing skills versus understanding concepts.
- Academic institutions of varying types continue to struggle in the process of mapping their curricula to any of these references. Guidance on this process would be valuable to the audience of this curricular volume – noting however, that the value of each reference is dependent upon the specific audience.

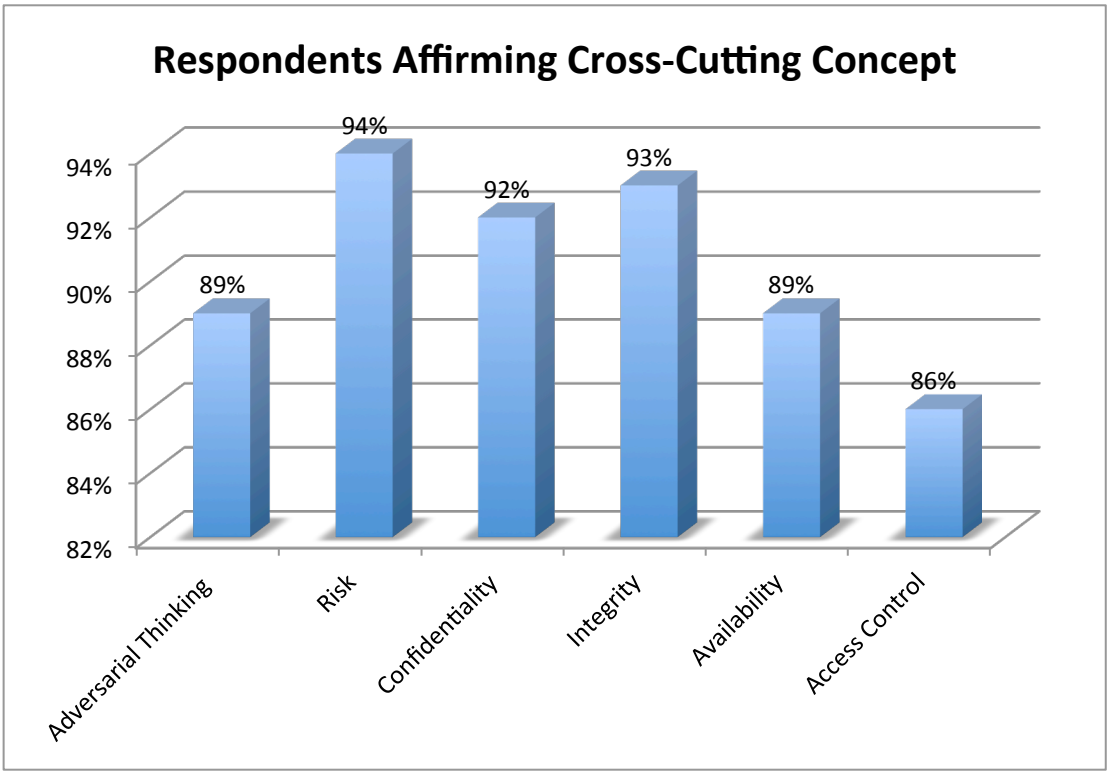
Cross-Cutting Concepts

Cross-Cutting Concepts bridge core ideas, practices and focus areas. Survey respondents were asked to review the Cross-Cutting Concepts listed below and (A) indicate if each listed Cross-Cutting Concepts should be included in the curricular volume; (B) suggest any changes to the definition of the Cross-Cutting Concepts and recommend the addition of Cross-Cutting Concepts not currently included.

Cross-Cutting Concepts:

1. Adversarial Thinking
2. Risk
3. Confidentiality
4. Integrity
5. Availability
6. Access control

(A) Percentage of respondents affirming Cross-Cutting Concept



(B) Summary Comments on Cross-Cutting Concepts

Survey respondents made several recommendations regarding the list of Cross-Cutting Concepts. The recommendations summarized below reflect the themes for each Cross-Cutting Concepts.

Adversarial Thinking

- Clarify the definition of adversarial thinking. Based on the definition, this concept could be foundational or it could be more oriented toward attacker/offensive thinking.

Risk

- Clarify the definition of risk. Is this concept related to IT management or considered more broadly with a business/organizational focus?

Confidentiality

- The concept is listed as cross-cutting and as a Core Idea. Clarify the distinction and the definition of the term.

Integrity

- The concept is listed as cross-cutting and as a Core Idea. Clarify the distinction and the definition of the term.

Availability

- The concept is listed as cross-cutting and as a Core Idea. Clarify the distinction and the definition of the term.

Access control

- Access control is not at the same level of importance as the other cross-cutting concepts.
- Clarify the definition of access control. Is it more than a mechanism or a technology?

Overall Comments

- Clarify the definition of cross-cutting concepts. What is the underlying principle that guides the content of this section? Is the intent to provide foundational knowledge or cross-cutting ideas? Rethink the level of the concepts and the breadth of topics included in the category.
- Consider adding ethics, privacy, non-repudiation, defense-in-depth/ layering and human-factors/people-oriented ideas.

Summary Comments on the Thought Model

General feedback on the thought model provided additional insight for the development process. Summary comments include:

- Clarify the intended audience of the curricular volume.
- Clarify the definitions and distinguish between the elements.
- Provide additional information on the content of each of the categories.
- Simplify the model.
- Provide a logical placement for emerging topics.

This report provides an overview of the feedback received from the stakeholder survey on the development of the first set of global cybersecurity curricular guidelines. The Joint Task Force continues to review and incorporate the detailed feedback into the development process.

The first draft of the Cybersecurity Curricular Volume will be released to the public in late 2016. Community engagement opportunities will be continuously updated on the csec2017.org website and community members are welcome to provide specific feedback to the JTF via that website at anytime.

The Joint Task Force will hold a Special Session at the ACM SIGCSE Meeting, March 8-11, 2017 in Seattle, Washington USA to discuss the draft document. Details on the specific time and location of the special session are forthcoming. Please plan to attend.