



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

June 6, 2012



ISOAG June 2012 Agenda

- | | | |
|-------------|---|--|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | ISSA Certifications | Jerry DeSanto, Chapter Exec. VP |
| III. | ISACA Certifications | Cathie Brown, Chapter President
John Karabaic, Dir of Certification |
| IV. | ISO Certification Program | Ed Miller, VITA |
| V. | Upcoming Events & Other Business | Michael Watson, VITA |
| VI. | Partnership Update | Bob Baskette, VITA, Eric Taylor,
Mike Clark, NG |

Jerry DeSanto
Manager Information
Services Security
Bon Secours Virginia
Health System

Security Certifications:

Choosing from an Alphabet Soup of
Options

Agenda

- Why Certify
 - Are Certifications Relevant?
 - Does the Type of Certifications Matter?
- CISSP
 - What is it
 - Who is it for
 - What's in it

Note: Opinions expressed are my own and do not necessarily reflect the opinions of my employer, (ISC)², ISSA etc.

Certifications Awarded

ICCP Certified Information Systems Analyst

HIPAA Academy Certified HIPAA Professional

CompTia A+

CompTia Security+

GIAC/SANS Global Information Security Fundamentals

(ISC)2 Certified Information Systems Security Professional

Degrees

NYU MPA Public Administration

Columbia University Political Science

Nassau Community College AA Marketing

Nassau Community College AS Business Administration

VCU MS Information Services (expected graduation 2013)

VCU Post Baccalaureate Certification Information Services

Why Certify

- Increased Earning Potential
- Increased Subject Matter Knowledge
- Increased Job Market Opportunities

Are Certifications Relevant

- Proof to employers as to who you are (Mike Dell or his slacker cousin)
 - Commitment
 - Diligence
 - Intelligence
- Knowledge growth during studying for exam

When to Seek a Certification

- Seeking a new job
- Remaining relevant in current job
- Want to change the type of work (different work than formal education)

The Type of Certification Matters

- Alphabet Soup of signature lines with meaningless certifications
- Even lame certifications can cost hundreds of dollars
- Meaningful Certs in the wrong area have minimal impact
- How to know which one should matter for you?
 - Job Postings
 - Recommendations from Friends
 - Certifications of co-workers

CISSP: Accredited by ANSI/ISO/IEC Standard 17024

- International Standards Organization – Representation from 157 countries
- American National Standards Institute – U.S. Representative to ISO
- ANSI/ISO/IEC Standard 17024
 - 88 countries participated
 - personnel certification system standard
- (ISC)² CISSP, CISSP-ISSAP, CISSP-ISSEP, CISSP-ISSMP, SSCP and CAP Credentials are all accredited under ANSI/ISO/IEC Standard 17024
- Establishes global benchmark for assessing and certifying personnel
- A global standard benefits
 - The information security profession
 - Businesses and governments
 - (ISC)² credential-holders



CISSP Requirements

- **The *Gold Standard* in information security certification is meant for professionals who:**
- Manage and enforce information security policies
- Are endorsed by another member of (ISC)²
- Pass a rigorous exam to assess knowledge, skills and abilities relevant to the CBK
- Real experience (next slide)

CISSP Experience Requirements

The CISSP requires a minimum of five years work experience in at least 2 of the 10 domains:

- *Access Control*
- *Software Development Security*
- *Business Continuity and Disaster Recovery Planning*
- *Cryptography*
- *Information Security Governance and Risk Management*
- *Legal, Regulations, Investigations and Compliance*
- *Operations Security*
- *Physical (Environmental) Security*
- *Security Architecture and Design*
- *Telecommunications and Network Security*

CISSP Exam

- \$599 (\$540 Early Registration)
- 6 Hours
- 250 Questions, of varying value
- Get pass fail results in 4-6 weeks
- Exam questions are different for same exam (domain focus)

CISSP Maintenance Requirements

- Earn minimum of 20 hours of Continuing Professional Education (CPEs) every year
- Total of 120 CPEs every three years for re-certification
- Annual Fees to (ISC)² of \$85
- Abide by the (ISC)² Code of Ethics

CISSP Ladder

The Associate of (ISC)²

- All the rigors of the CISSP for someone who does not have the professional experience requirements.
- Valid for a maximum of six years from the date (ISC)² notifies you that you have passed the exam, within which time, you'll need to obtain the required experience and submit the required endorsement form.

CISSP Ladder

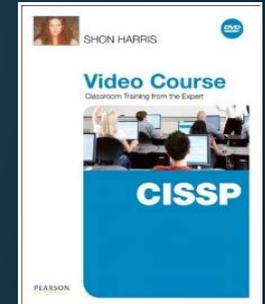
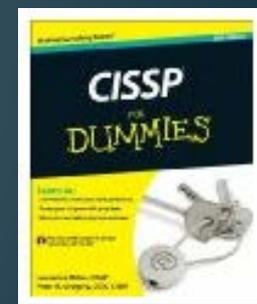
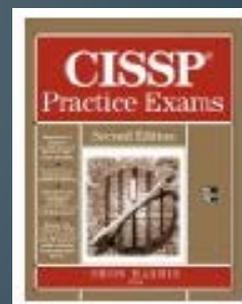
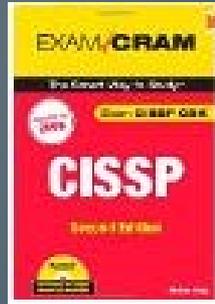
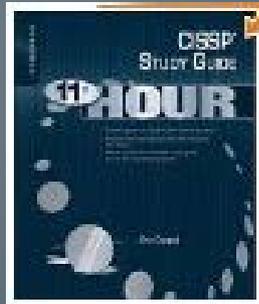
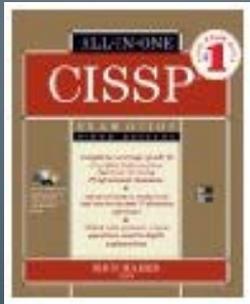
Having the CISSP credential allows users to complete three concentrations that demonstrate proven capabilities and subject-matter expertise beyond the CISSP credential.

The three concentrations are:

- ISSAP: architecture
- ISSMP : management
- ISSEP: engineering

My CISSP Study Tools

- Books
- Website
- Video



CISSP Study Tools



ISSA Training

- 3 hour sessions once a week for 13 weeks
- Covers the ten CISSP domains
- Final session is dedicated to a practice CISSP exam and additional review.
- Taught by CVA ISSA members who are experts in that domain
- Fee: \$450.00 (Membership in the Central VA ISSA is required)

Q&A



ISACA®

Trust in, and value from, information systems

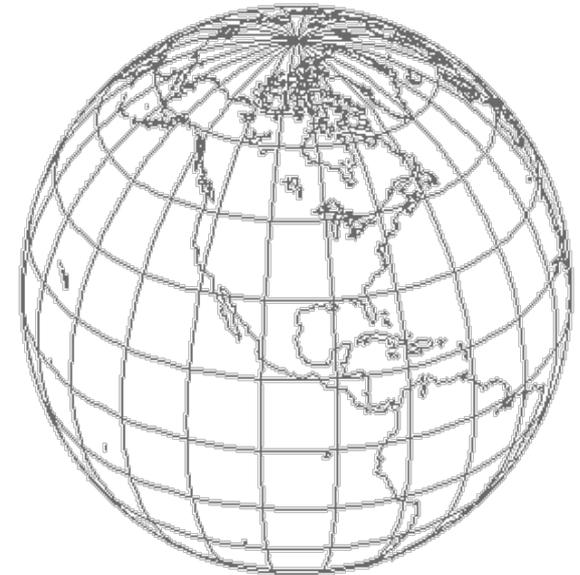
www.isaca.org

CISA/CISM/CGEIT/CRISC Programs Overview



www.isaca.org/certification

- Founded in 1969 as the EDP Auditors Association
- Since 1978, CISA has been a globally accepted standard of competency among IS audit, control, assurance and security professionals
- More than 95,000 members in over 160 countries
- More than 190 chapters worldwide



- The American National Standards Institute (ANSI) has accredited the CISA[®], CISM[®] and CGEIT[®] certifications under ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons. ANSI, a private, nonprofit organization, accredits other organizations to serve as third-party product, system and personnel certifiers. ISO/IEC 17024 specifies the requirements to be followed by organizations certifying individuals against specific requirements.
- This is both an international and US accreditation. It is based on an international standard but implemented by ANSI to be recognized in the US and other countries that enter into an arrangement with ANSI. This is in keeping with the purpose of ISO/IEC 17024 to begin standardization of accreditation of personnel certification agencies around the world.
- Accreditation by ANSI signifies that ISACA's procedures meet ANSI's essential requirements for openness, balance, consensus and due process.

CISA Certification Details



www.isaca.org/cisa

Why Become A CISA?

- ***Enhanced Knowledge and Skills***
 - To demonstrate your willingness to improve your technical knowledge and skills
 - To demonstrate to management your proficiency and commitment toward organizational excellence
- ***Career Advancement***
 - To obtain credentials that employers seek
 - To enhance your professional image
- ***Worldwide Recognition***
 - To be included with more than 90,000 other professionals who have gained the CISA designation worldwide

- Nearly 2,500 are employed in organizations as the CEO, CFO or equivalent executive position.
- More than 2,000 serve as chief audit executives, audit partners or audit heads.
- Over 2,200 serve as CIOs, CISOs, or chief compliance, risk or privacy officers.
- Almost 8,200 are employed as security directors, managers or consultants and related staff.
- More than 10,400 are employed as IT directors, managers, consultants and related staff.
- Nearly 27,000 serve as audit directors, managers or consultants and auditors (IT and non-IT).
- Over 7,800 are employed in managerial, consulting or related positions in IT operations or compliance.

Recent CISA Program Recognition

- SC Magazine selected CISA again as a finalist of the 2012 “Best Professional Certification Program in the Professional Awards category. CISA was named a finalist by a panel of 22 chief information security officers (CISOs) at major corporations and large public-sector organizations.
- CISA was named in the top five of Foote Partners’ 2011 semiannual “HOT LIST Forecast” of IT skills and certifications that will increase in value over the next six months.

Recent CISA Program Recognition *(continued)*

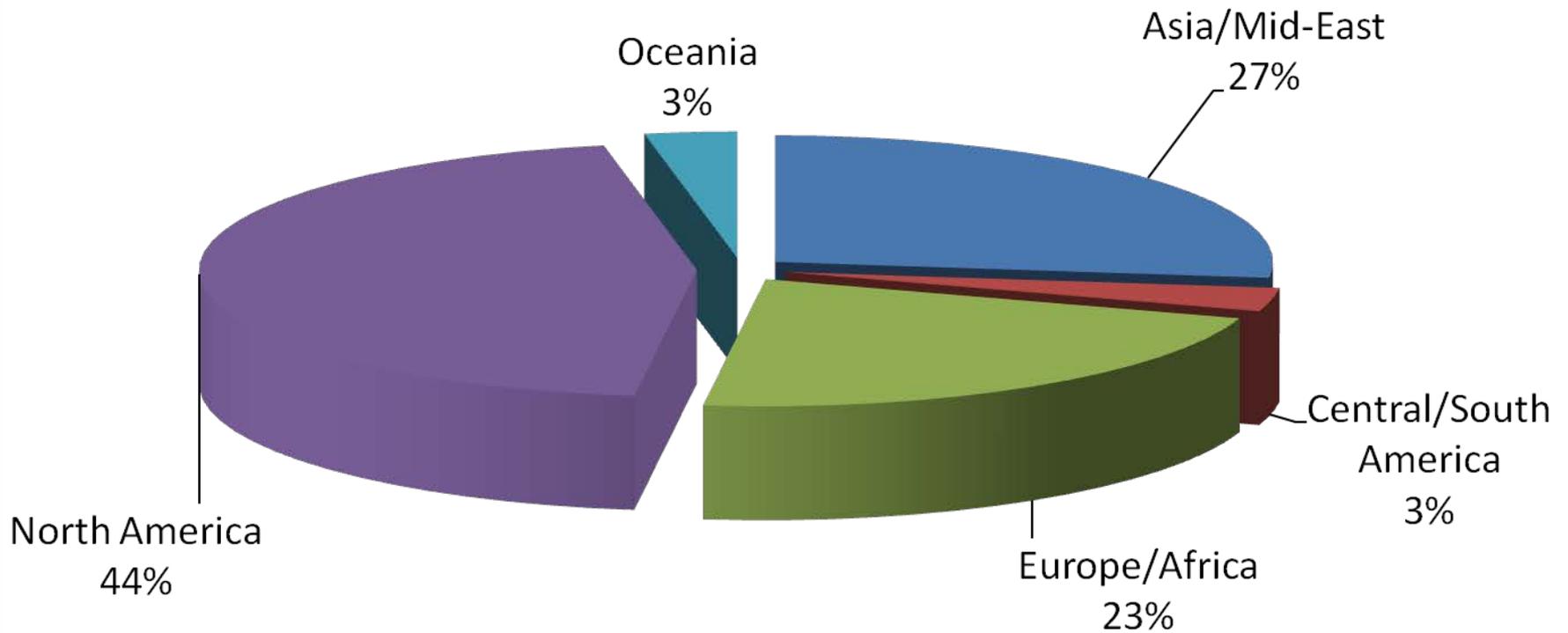
- The World Lottery Association (WLA) has recognized ISACA's CISA and CISM as certifications that are required for someone to be a WLA auditor. The WLA's "*Guide to Certification for the WLA Security Control Standard*" details that a certification auditor seeking accreditation from the WLA to conduct WLA SCS certification audits should be actively involved in the business of information systems, be either ISO/IEC 27001:2005 lead-auditor certified, or an IT security expert or IT auditor, as certified by an internationally recognized certification body, possess experience in the lottery sector of reasonable duration and hold one or more designations of which the CISA and CISM certifications qualify.

Other CISA Program Recognition

- The US Department of Defense includes CISA in its list of approved certifications for its information assurance professionals.
- In India, both the National Stock Exchange and the Indian Computer Emergency Response Team (CERT-IN) require CISA certification for employees to carry out security audits.
- All assistant examiners employed by the Federal Reserve Banks must pass the CISA examination before they are eligible for commissioning.
- The National Association of Insurance Companies (NAIC) includes CISA among the approved certifications for qualified IT examiners.

More information may be found at www.isaca.org/recognitions

CISAs by Area



CISA Job Practice Areas

(Effective 2011)

1. *The Process of Auditing Information Systems – 14%*

Provide audit services in accordance with IT audit standards to assist the organization in protecting and controlling information systems.

2. *Governance and Management of IT – 14%*

Provide assurance that the necessary leadership and organization structure and processes are in place to achieve objectives and to support the organization's strategy.

3. *Information Systems Acquisition, Development and Implementation – 19%*

Provide assurance that the practices for the acquisition, testing and implementation of information systems meet the organization's strategies and objectives.

CISA Job Practice Areas

(Effective 2011) *(continued)*

4. *Information Systems Operations, Maintenance and Support – 23%*

Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives.

5. *Protection of Information Assets – 30%*

Provide assurance that the organization's security policies, standards, procedures, and controls ensure the confidentiality, integrity, and availability of information assets.

For complete details, visit www.isaca.org/cisajobpractice

CISA Certification Requirements

- Earn a passing score on the CISA Exam. (CISA exam is offered in 11 languages.)
- Have a minimum of five years of verifiable IS audit, control or security experience (substitutions available)
- Submit the CISA application and receive approval
- Adhere to ISACA's *Code of Professional Ethics*
- Abide by *IS Auditing Standards* as adopted by ISACA
- Comply with *CISA Continuing Professional Education Policy*

CISM Certification Details



www.isaca.org/cism

CISM Certification Current Facts

- More than 16,000 CISM[®]s worldwide
- The CISM exam is offered in 4 languages (English, Japanese, Korean and Spanish) in over 240 locations

Why Become a CISM?

Enhanced Knowledge and Skills

- To demonstrate your willingness to improve your technical knowledge and skills

Career Advancement

- To demonstrate to management your commitment toward organizational excellence
- To obtain credentials that employers seek
- To enhance your professional image

Worldwide Recognition

- To be included with other professionals who have gained worldwide recognition

What makes CISM Unique?

- Designed for information security managers exclusively
- Criteria and exam developed from job practice analysis validated by information security managers
- Experience requirement includes information security management

What is the CISM Target Market?

Individuals who design, implement and manage an enterprise's information security program.

- Security managers
- Security directors
- Security officers
- Security consultants
- Security staff

Recent CISM Recognition

- GovInfoSecurity.com shows CISM as one of the top 5 security certifications for 2011.
- The 2010 Information Career Trends Survey, conducted by the Information Security Media Group, found CISM to be one of the three most sought-after certifications for security professionals. According to ISMG, CISM is one of the two certifications becoming "minimum standards in the profession."

Recent CISM Recognition

- The World Lottery Association (WLA) has recognized ISACA's CISA and CISM as certifications that are required for someone to be a WLA auditor. The WLA's "Guide to Certification for the WLA Security Control Standard" details that a certification auditor seeking accreditation from the WLA to conduct WLA SCS certification audits should be actively involved in the business of information systems, be either ISO/IEC 27001:2005 lead-auditor certified, or an IT security expert or IT auditor, as certified by an internationally recognized certification body, possess experience in the lottery sector of reasonable duration and hold one or more designations of which the CISA and CISM certifications qualify.

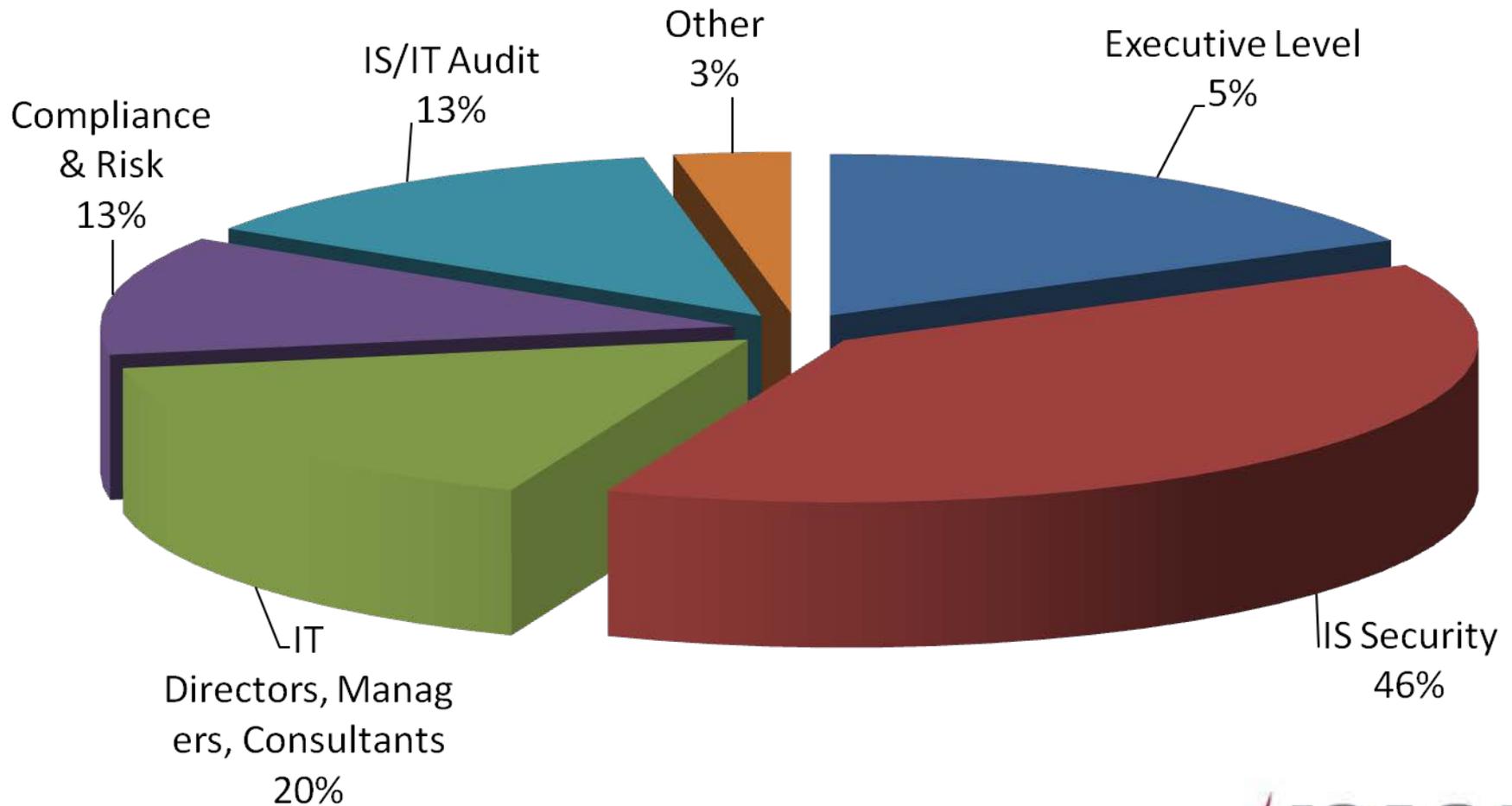
Recent CISM Recognition

(continued)

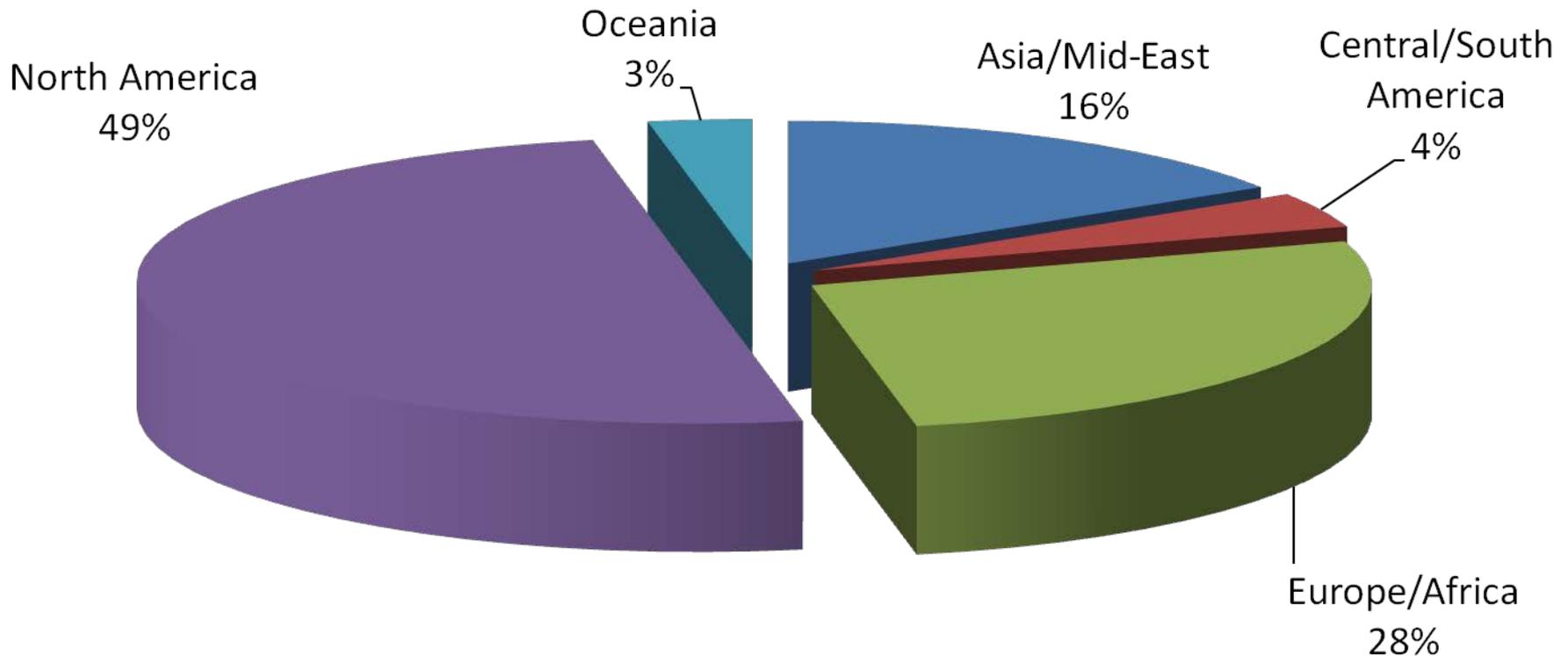
- The CISM Certification Program has again been selected as a finalist in *SC Magazine's* 2012 Best Professional Certification Program category.
- CISM was recently recognized at the Hong Kong ICT Awards 2011 with the Certificate of Merit under the “Best Professional Development (ICT Professional) Award.” The Hong Kong ICT Awards were established in 2006 under a collaborative effort among the industry, academia and the government. The Certificate of Merit is the award that all of the finalists in each category receive.
- The US Department of Defense includes CISM in its list of approved certifications for its information security professionals.

More information may be found at www.isaca.org/recognitions

CISMs by Job Title



CISMs by Geographic Area



- 1. Information Security Governance (24%)** – Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly.
- 2. Information Risk Management and Compliance (33%)** – Manage information risk to an acceptable level to meet the business and compliance requirements of the organization.
- 3. Information Security Program Development and Management (25%)** – Establish and manage the information security program in alignment with the information security strategy.
- 4. Information Security Incident Management (18%)** – Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact

For more details visit www.isaca.org/cismjobpractice

CISM Certification Requirements

- Earn a passing score on the CISM exam
- Submit verified evidence of a minimum of five years of information security management work experience (covering 3 of the 4 job practice domains)
- Submit completed CISM application within 5 years of passing exam and receive approval
- Adhere to the *ISACA Code of Professional Ethics*
- Comply with the *CISM Continuing Professional Education Policy*

CGEIT Certification Details



www.isaca.org/cgeit

Market Need for CGEIT

- **Individual**
 - ✓ Defines the roles and responsibilities of professionals performing IT governance work and recognizes their professional knowledge and competencies; skill-sets; abilities and experiences
- **Enterprise**
 - ✓ Supports through the demonstration of a visible commitment to excellence in IT governance practices
- **Business**
 - ✓ Increases the awareness of IT governance good practices and issues
- **Profession**
 - ✓ Supports those that provide IT governance management, advisory or assurance direction and strategy

CGEIT: Who is it for?

The CGEIT certification is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices. It is designed for professionals who have management, advisory, or assurance responsibilities as defined by the CGEIT Job Practice consisting of IT governance related task and knowledge statements.

CGEITs in the Workplace

- Nearly 400 are employed in organizations as the CEO, CFO or equivalent executive position.
- Almost 200 serve as chief audit executives, audit partners or audit heads.
- Over 500 serve as CIOs, CISOs, or chief compliance, risk or privacy officers.
- Almost 600 are employed as security directors, managers or consultants and related staff.
- Nearly 1,000 are employed as IT directors, managers, consultants and related staff.
- More than 950 serve as audit directors, managers or consultants and related staff.
- Over 550 are employed in managerial, consulting or related positions in IT operations or compliance.

Recent CGEIT Recognition

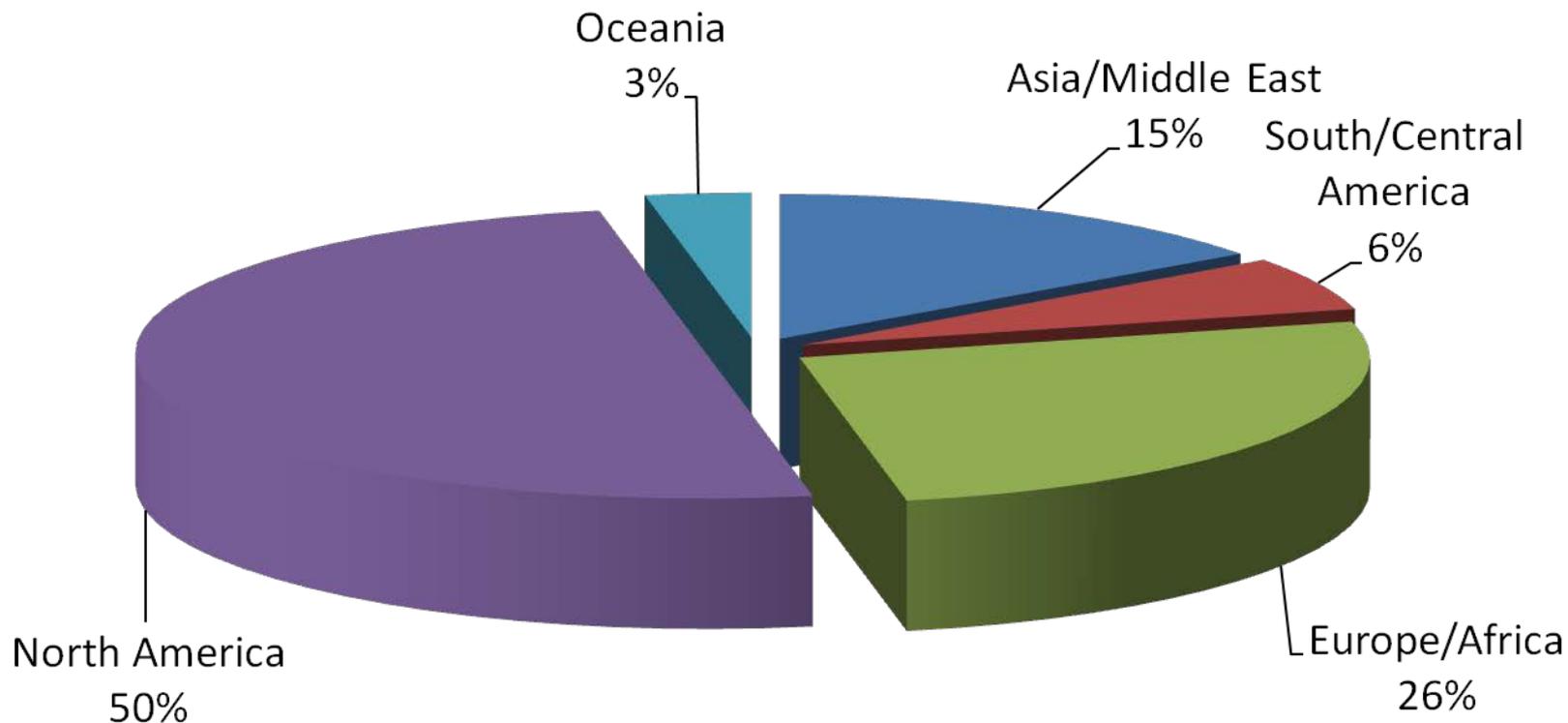
- ISACA certification programs have recently been recognized for experience and education credits by the International *itSMF* for their new *prISM* certification program. The CGEIT certification relates to credits at the distinguished professional level.
- CGEIT was named a finalist for the 2011 *SC Magazine* Best Professional Certification Program Award.

More information may be found at www.isaca.org/recognitions



Certified in the
Governance of
Enterprise IT[®]
An ISACA[®] Certification

CGEITs by Geographical Area



1. *IT Governance Framework (25%)*

Define, establish and maintain an IT governance framework (leadership, organizational structures and processes) to: ensure alignment with enterprise governance; control the business information and information technology environment through the implementation of good practices; and assure compliance with external requirements.

2. *Strategic Alignment (15%)*

Ensure that IT enables and supports the achievement of business objectives through the integration of IT strategic plans with business strategic plans and the alignment of IT services with enterprise operations to optimize business processes.

3. Value Delivery (15%)

Ensure that IT and the business fulfill their value management responsibilities: IT-enabled business investments achieve the benefits as promised and deliver measurable business value both individually and collectively, that required capabilities (solutions and services) are delivered on-time and within budget, and that IT services and other IT assets continue to contribute to business value.

4. Risk Management (20%)

Ensure that appropriate frameworks exist and are aligned with relevant standards to identify, assess, mitigate, manage, communicate and monitor IT-related business risks as an integral part of an enterprise's governance environment.

5. Resource Management (13%)

Ensure that IT has sufficient, competent and capable resources to execute current and future strategic objectives and keep up with business demands by optimizing the investment, use and allocation of IT assets.

6. Performance Measurement (12%)

Ensure that business-supporting IT goals/objectives and measures are established in collaboration with key stakeholders and that measurable targets are set, monitored and evaluated.

For more details visit www.isaca.org/cgeitjobpractice

CGEIT Experience Requirements

- Earn a passing score on the CGEIT exam
- Submit verified evidence of the five year experience requirement as defined by the *CGEIT Job Practice*
- Submit the CGEIT application and receive approval
- Adhere to the *ISACA Code of Professional Ethics*
- Comply with the *CGEIT Continuing Education Policy*

Certified in Risk and Information Systems Control[™]



www.isaca.org/crisc

Designed exclusively for risk and information controls personnel who:

- Identify, assess and analyze risk
- Design, implement and maintain controls to mitigate risk
- Respond to risk events

Why Become a CRISC?

Enhanced Knowledge and Skills

- To demonstrate your willingness to improve your technical knowledge and skills

Career Advancement

- To demonstrate to management your commitment toward organizational excellence
- To obtain credentials that employers seek
- To enhance your professional image

Worldwide Recognition

- To be included with other professionals who have gained worldwide recognition

CRISC in the Workplace

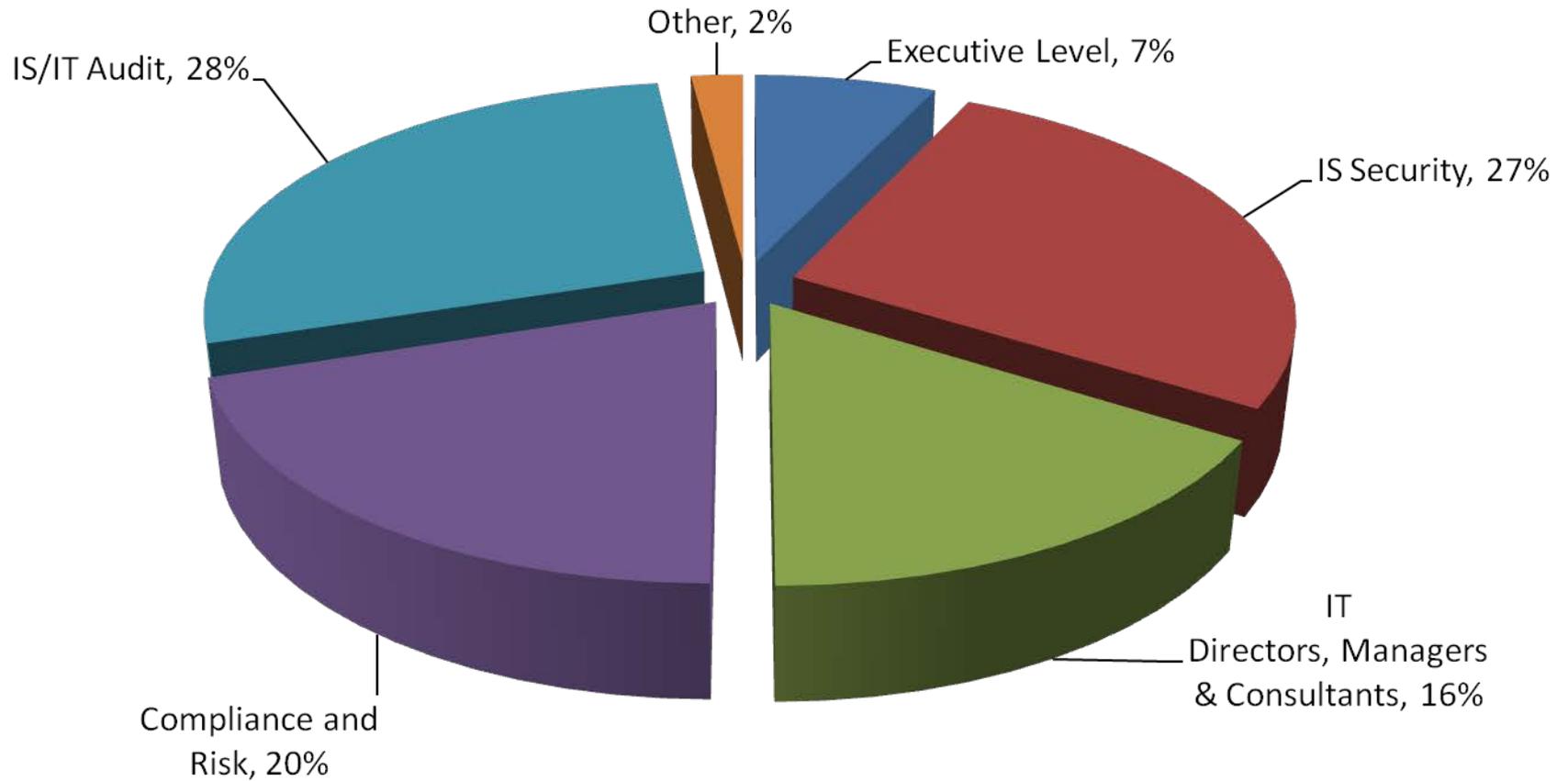
- Nearly 600 are employed in organizations as the CEO, CFO or equivalent executive position.
- More than 400 serve as chief audit executives, audit partners or audit heads.
- Over 1,200 serve as CIOs, CISOs, or chief compliance, risk or privacy officers.
- More than 3,500 are employed as security directors, managers or consultants and related staff.
- More than 2,200 are employed as IT directors, managers, consultants and related staff.
- Nearly 4,400 serve as audit directors, managers or consultants and related staff.
- Over 2,900 are employed in managerial, consulting or related positions in IT operations or compliance.

Recent CRISC Program Recognitions

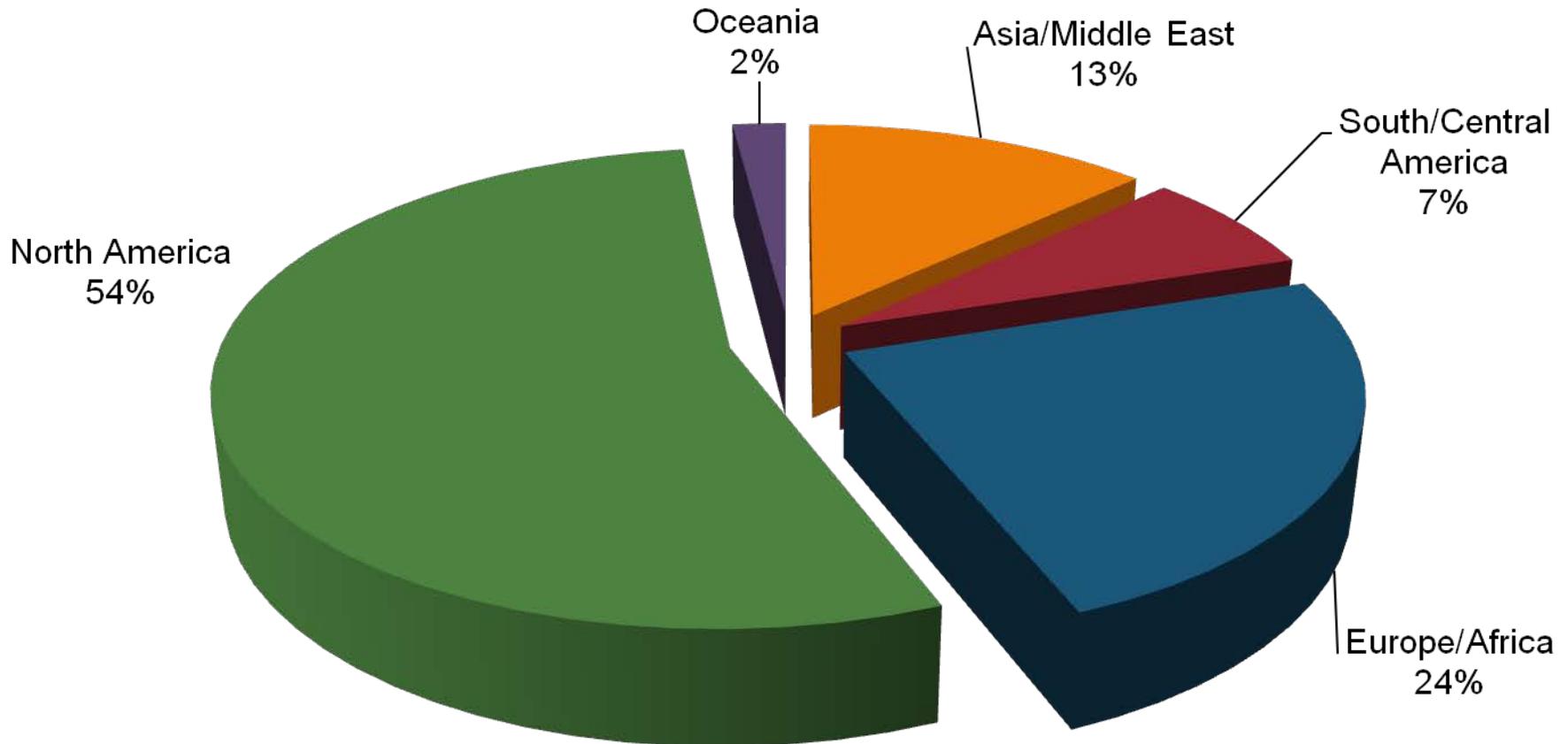
- ISACA certification programs have recently been recognized for experience and education credits by the International *itSMF* for their new *priSM* certification program. The CRISC certification relates to credits at the professional level.
- The State of West Virginia Office of Information Security and Controls is using the 5 CRISC domains and task statements to develop a checklist for use in risk assessments for HIPAA compliance. The task statements will be mapped to NIST standards. This checklist will be used by the West Virginia state government and its business associates who are handling West Virginia collected Protected Health Information (PHI).

More information may be found at www.isaca.org/recognitions

CRISCs by Job Title



CRISCs by Area



Domain 1—Risk Identification, Assessment and Evaluation (31%)

Identify, assess and evaluate risk to enable the execution of the enterprise risk management strategy.

Domain 2—Risk Response (17%)

Develop and implement risk responses to ensure that risk issues, opportunities and events are addressed in a cost-effective manner and in line with business objectives.

Domain 3—Risk Monitoring (17%)

Monitor risk and communicate information to the relevant stakeholders to ensure the continued effectiveness of the enterprise's risk management strategy.

Domain 4—IS Control Design and Implementation (17%)

Design and implement IS controls in alignment with the organisation's risk appetite and tolerance levels to support business objectives.

Domain 5—IS Control Monitoring and Maintenance (18%)

Monitor and maintain IS controls to ensure they function effectively and efficiently.

CRISC Certification Requirements

- Earn a passing score on the CRISC exam
- Submit verified evidence of a minimum of 3 years of risk and information systems controls experience (covering 3 of the 5 job practice domains)
- Submit completed CRISC application within 5 years of passing exam and receive approval
- Adhere to the *ISACA Code of Professional Ethics*
- Comply with the *CRISC Continuing Professional Education Policy*

CISA, CISM, CGEIT and CRISC Exam Details



CISA[®] Certified Information Systems Auditor[®]
An ISACA[®] Certification



CISM[®] Certified Information Security Manager[®]
An ISACA[®] Certification



CGEIT[®] Certified in the Governance of Enterprise IT[®]
An ISACA[®] Certification



CRISC[™] Certified in Risk and Information System Controls
An ISACA[®] Certification

Administration of the Exams

2012 Exam Dates:

Saturday 9 June 2012

Saturday 8 December 2012

- The exams are offered at over 240 locations worldwide
- Offered in every city where there is an ISACA chapter or a large interest in individuals sitting for the exam
- Passing mark of 450 on a common scaled scale of 200 to 800

2012 Registration Fees: 9 June 2012

Early Registration - On or before 8 February 2012:

- ISACA Member: US \$445.00
- Non-Member: US \$595.00

Final Registration – After 8 February, but on or before 4 April 2012:

- ISACA Member: US \$495.00
- Non-Member: US \$645.00

Register Online at www.isaca.org/examreq and save \$\$

- Online registration via the ISACA web site is encouraged, as candidates will save US \$50. Non-members can join ISACA at the same time, which maximizes their savings.

Exam registration fees must be paid in full to sit for the exams. Those whose exam registration fees are not paid will not be sent an exam admission ticket and their registration will be cancelled.

2012 Registration Fees: 8 December 2012

Early Registration - On or before 15 August 2012:

- ISACA Member: US \$445.00
- Non-Member: US \$595.00

Final Registration – After 15 August, but on or before 3 October 2012:

- ISACA Member: US \$495.00
- Non-Member: US \$645.00

Register Online at www.isaca.org/examreq and save \$\$

- Online registration via the ISACA web site is encouraged, as candidates will save US \$50. Non-members can join ISACA at the same time, which maximizes their savings.

Exam registration fees must be paid in full to sit for the exams. Those whose exam registration fees are not paid will not be sent an exam admission ticket and their registration will be cancelled.

Bulletin of Information (BOI) and Registration Form

- There is a *Bulletin of Information* for each exam administration for each exam.
- Can be downloaded from the ISACA web site at:
www.isaca.org/cisaboi, www.isaca.org/cismboi,
www.isaca.org/cgeitboi and www.isaca.org/criscboi.

Bulletin includes:

- Requirements for certification
- Exam description
- Registration instructions and deadline dates
- Test date procedures
- Score reporting
- Test center locations
- Registration forms

Types of Questions on the Exams

- The CISA, CISM and CRISC exams consist of 200 multiple choice questions administered over a four-hour period.
- The CGEIT exam consists of 120 multiple choice questions administered over a four-hour period.
- Questions are designed to test practical knowledge and experience
- Questions require the candidate to choose one best answer
- Every question or statement has four options (answer choices)

Quality of the Exam Ensured by:

- **Job Analysis Study:** determines content
- **Test Development Standards:** ensures high standards for the development and review of questions
- **Review Process:** provides two reviews of questions by independent committees before acceptance into pool
- **Periodic Pool Cleaning:** ensures that questions in the pool are up-to-date by continuously reviewing questions
- **Statistical Analysis of Questions:** ensures quality questions and grading by analyzing exam statistics for each language

CISA, CISM, CGEIT and CRISC Continuing Professional Education (CPE) Policy Details

Continuing Professional Education (CPE) Requirements

Certification is renewed annually to those who:

- Report a minimum of 120 hours of continuing professional education (CPE) for each fixed three-year period, with a minimum of 20 hours in each year.
- Report hours annually, in the year they are earned. Hours are reported annually during the renewal process.
- Pay annual certification maintenance fee
- Comply with the ISACA Code of Professional Ethics

ISACA membership provides a number of activities of which to earn CPE. To learn more about ISACA membership visit

www.isaca.org/join.

ISACA Code of Professional Ethics

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting the profession or the Association.

ISACA Code of Professional Ethics

(continued)

Members and ISACA certification holders shall:

4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

www.isaca.org/ethics

ISACA Member Benefits

- Professional Development (discounted fees)
 - Certifications (CISA, CISM, CGEIT, CRISC)
 - e-Learning and Career Center
 - Conferences and Training
 - Local Chapter Events
 - Bookstore
- Research and Knowledge (complimentary)
 - VALIT, RISKIT and COBIT Frameworks
 - Whitepapers
 - ISACA Journal and Newsletters

- Community and Leadership
 - Connections with a global community of more than 95,000 peers
 - Networking (face-to-face and online)
 - Leadership opportunities
 - Local Chapter Level
 - International Level

*Contact us for additional
information about the ISACA
Virginia Chapter*

- Cathie Brown, CGEIT, PMP, CISM, CISSP
President, ISACA Virginia Chapter
(434) 665-0345
president@isaca-va.org
- Scott Hammer, CISM, CSIRC, PMP
Vice President, ISACA Virginia Chapter
(804) 306-9685
vicepresident@isaca-va.org
- John Karabaic, CISM, CPP
Past Certification Director, ISACA Virginia Chapter
(804) 677-0449
Johnkarabaic@comcast.net

Want to know more?
Please contact us at:

ISACA
3701 Algonquin Road
Suite 1010
Rolling Meadows, IL 60008
USA

- Phone: +1.847.660.5660
- Fax: +1.847.253.1443
- E-mail: certification@isaca.org
- Web site: www.isaca.org



ISO Certification Program

Ed Miller
Security Analyst

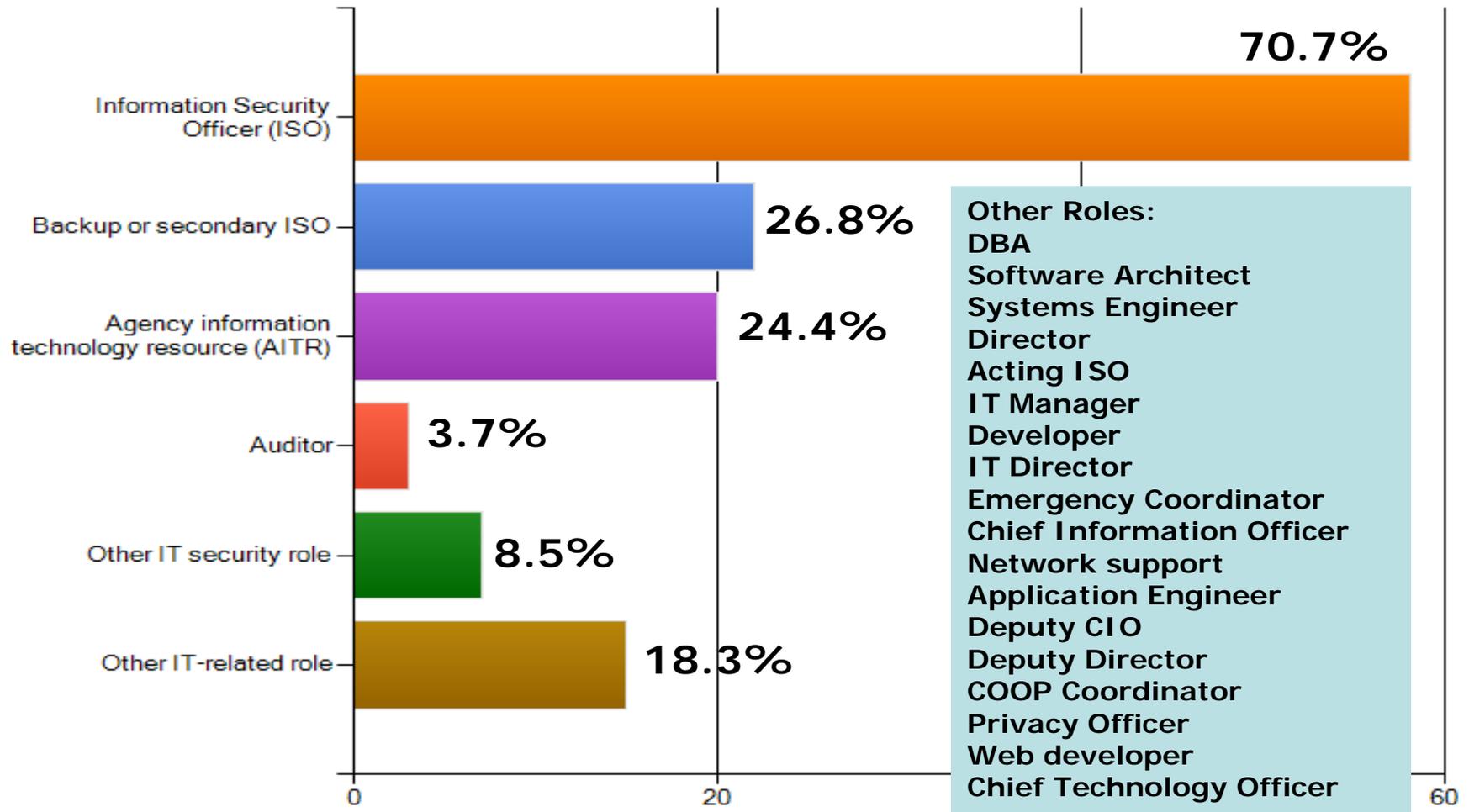


Survey of our ISO's

- We recently concluded a survey of ISO's/Backup ISO's.
- The objective of the survey was to determine the prevalence of IT security certifications held by Commonwealth ISO's and to identify some of the training needs and concerns of the group.
- The survey went to approximately 150 names. We received a response from 78 people.
- Here is what you said:

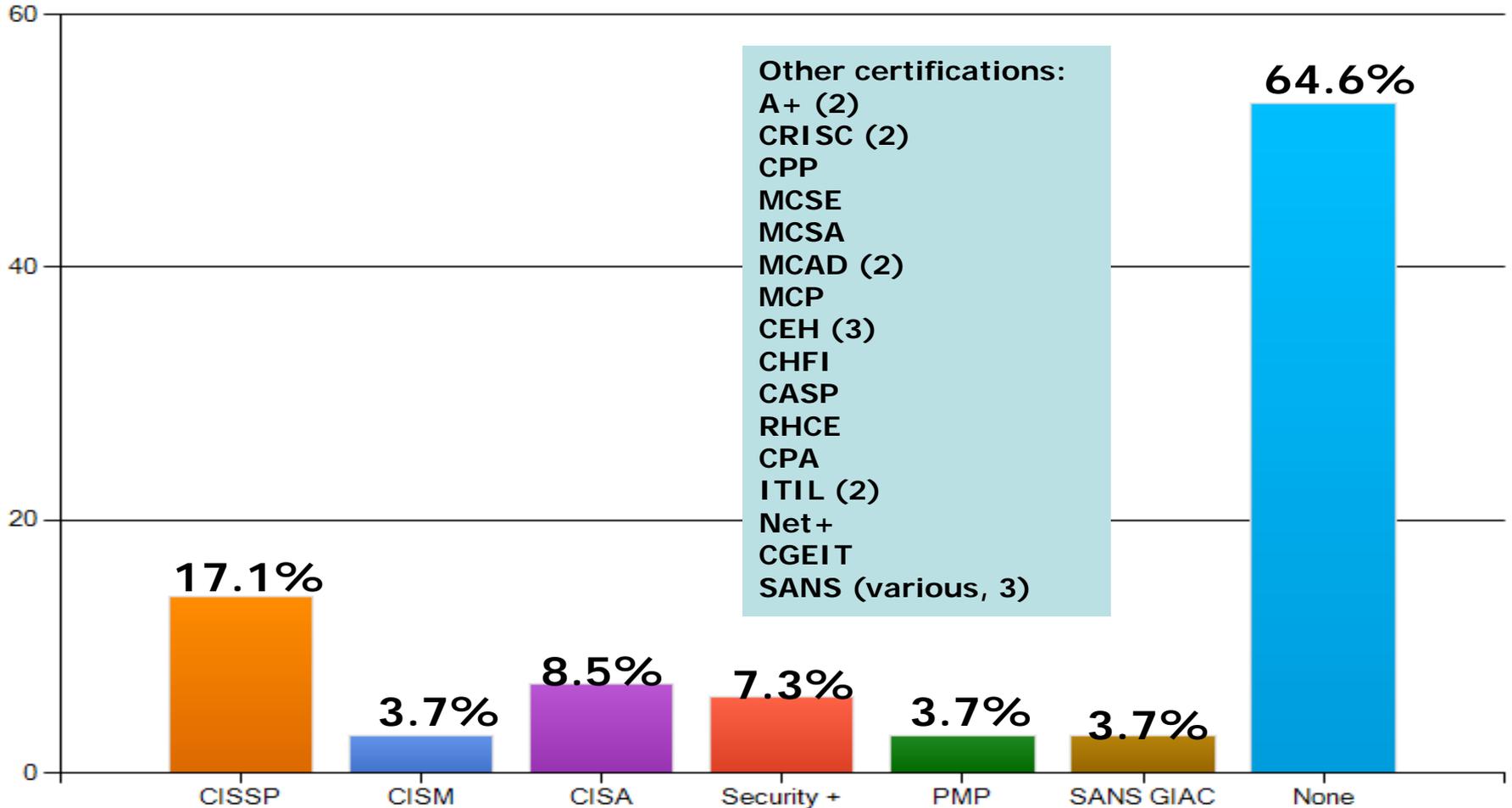


What is your role at your agency (check all that apply)?



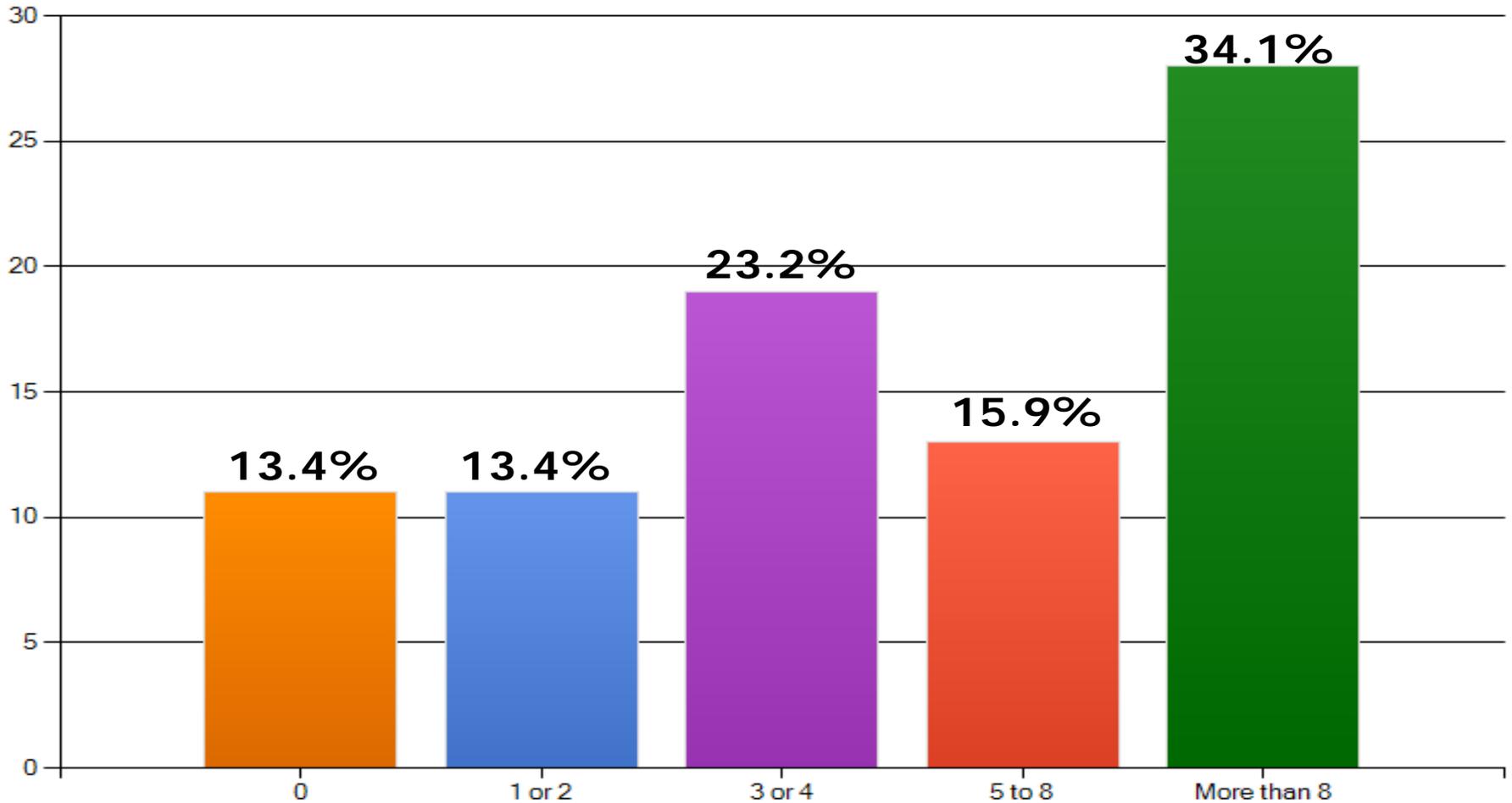


What professional certifications do you currently hold and maintain (including vendor specific, e.g. Cisco, Redhat, Microsoft, etc.)?

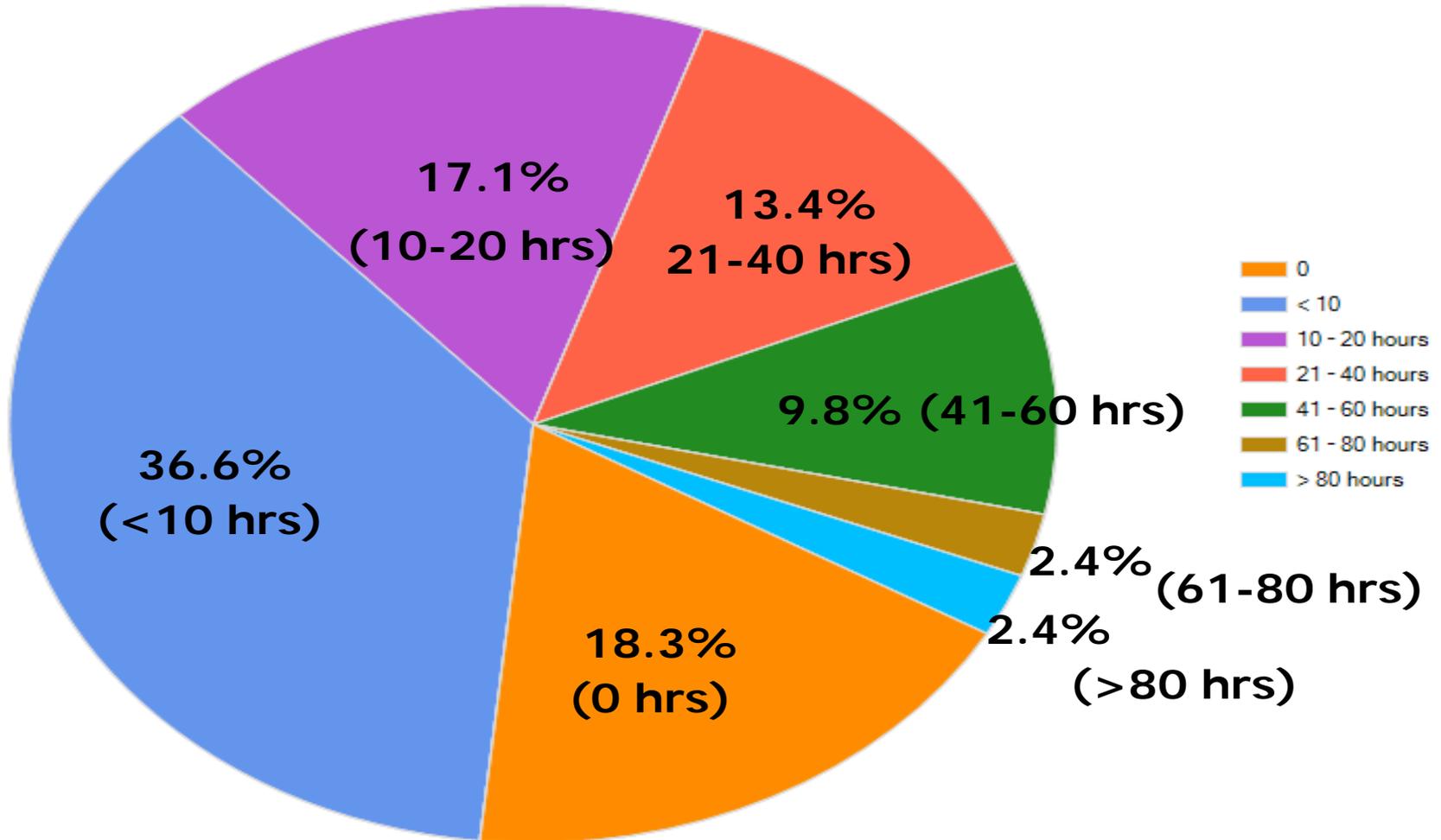




How many information security officer advisory group (ISOAG) meetings (in person or by webinar) per year do you attend?

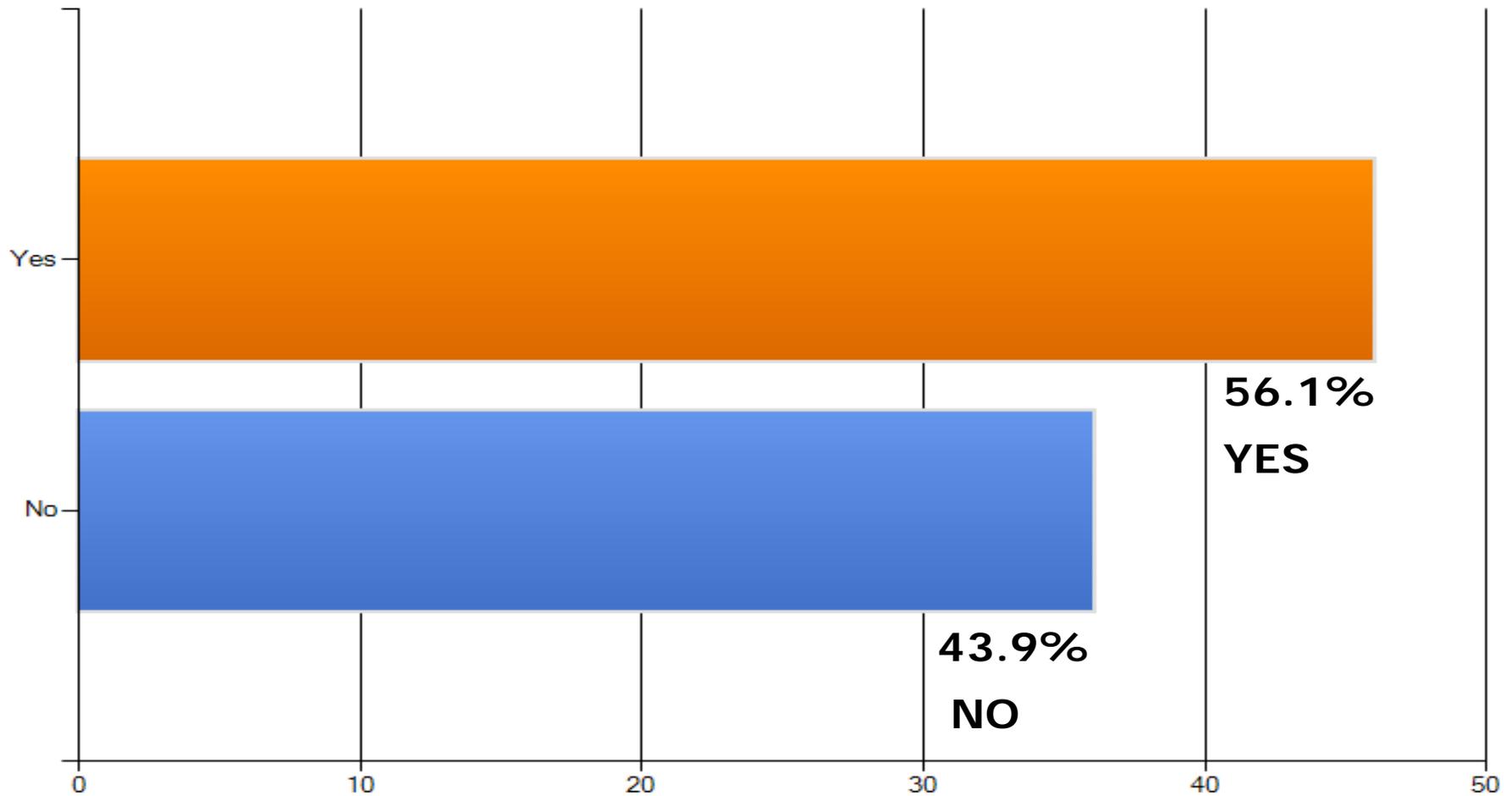


How many hours do you spend attending IT security seminars or conferences (other than ISOAG meetings or professional chapter meetings) each year?

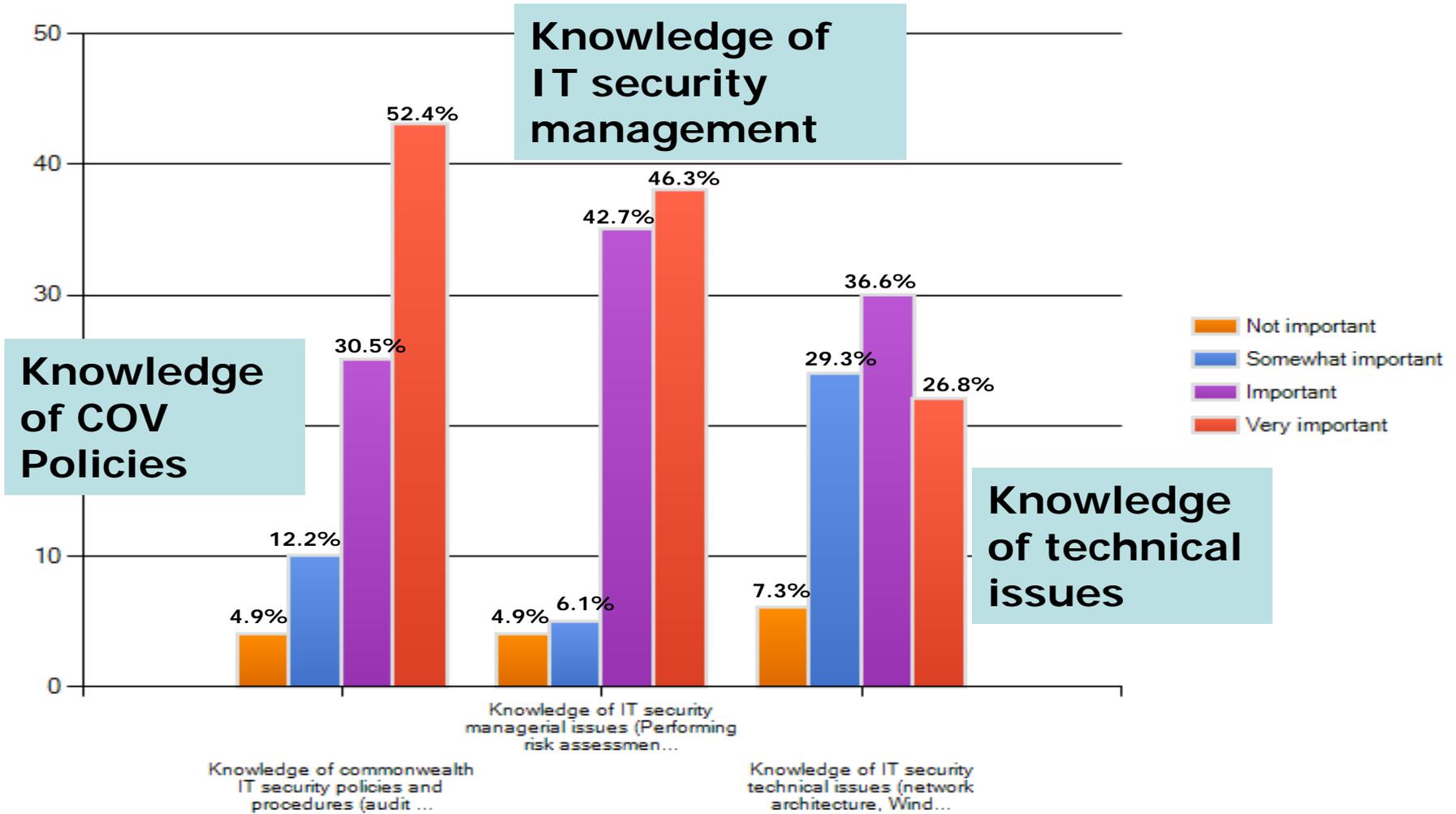




Do you think it would benefit you and/or your agency to have a Commonwealth administered ISO certification?

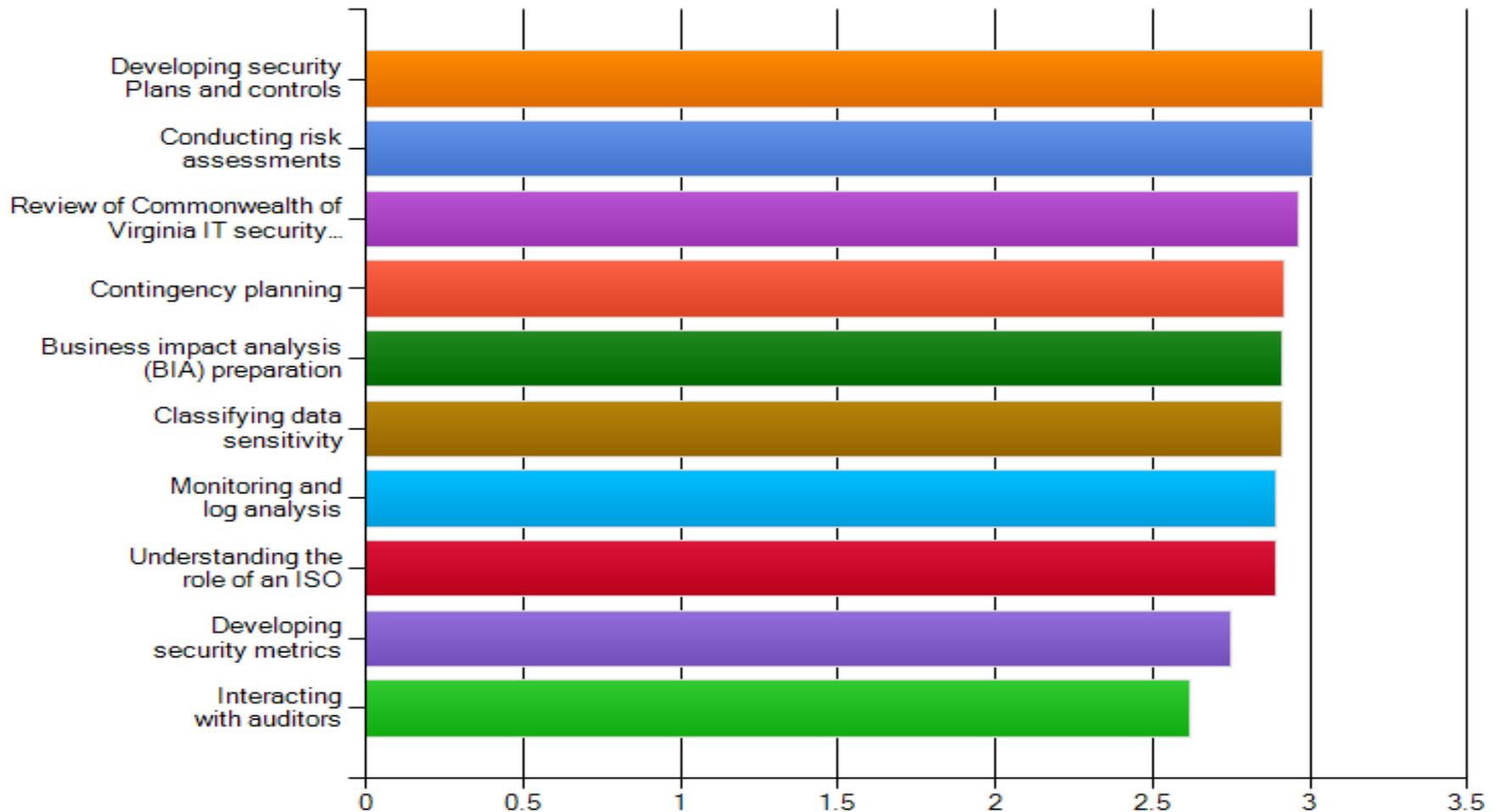


Please rank the following criteria that could be used to evaluate the knowledge needed by a commonwealth ISO in terms of importance.



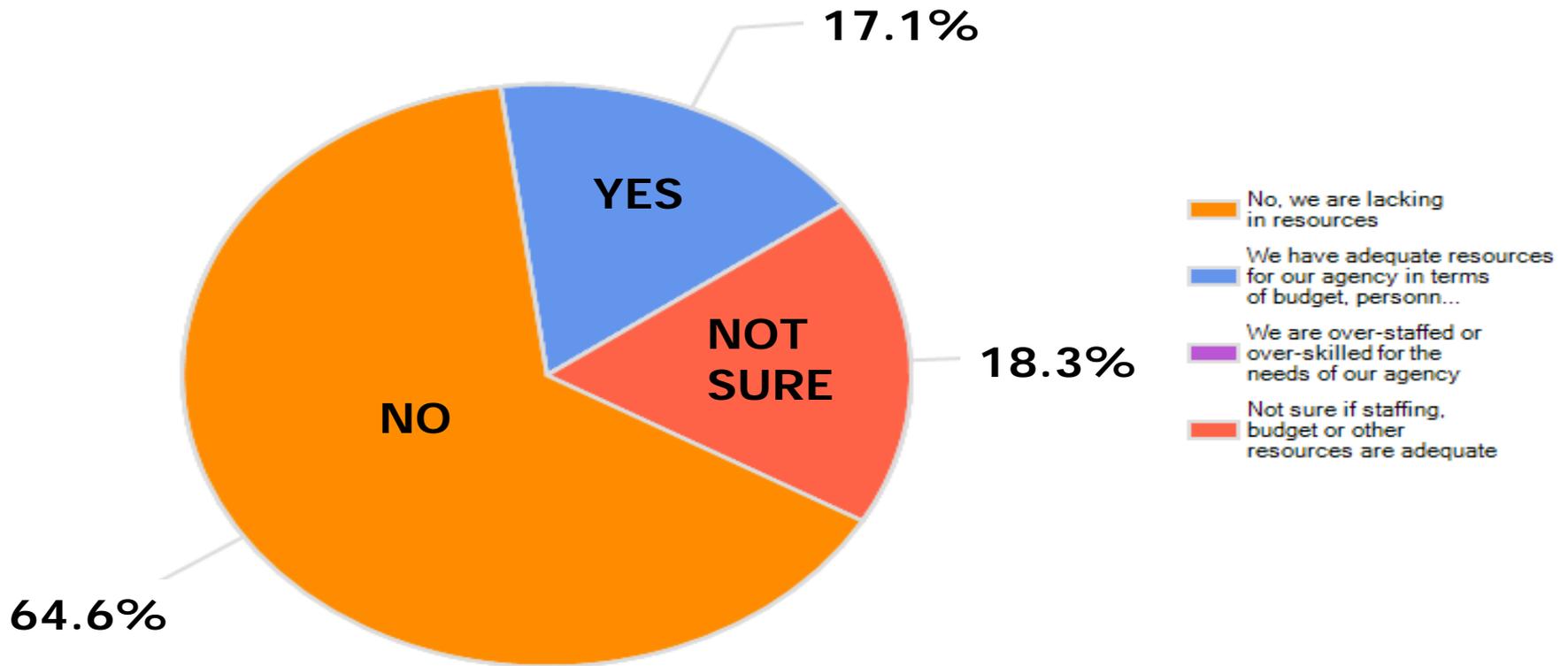


Rank the following subjects as potential course topics that you would find useful or beneficial to support your role at your agency:



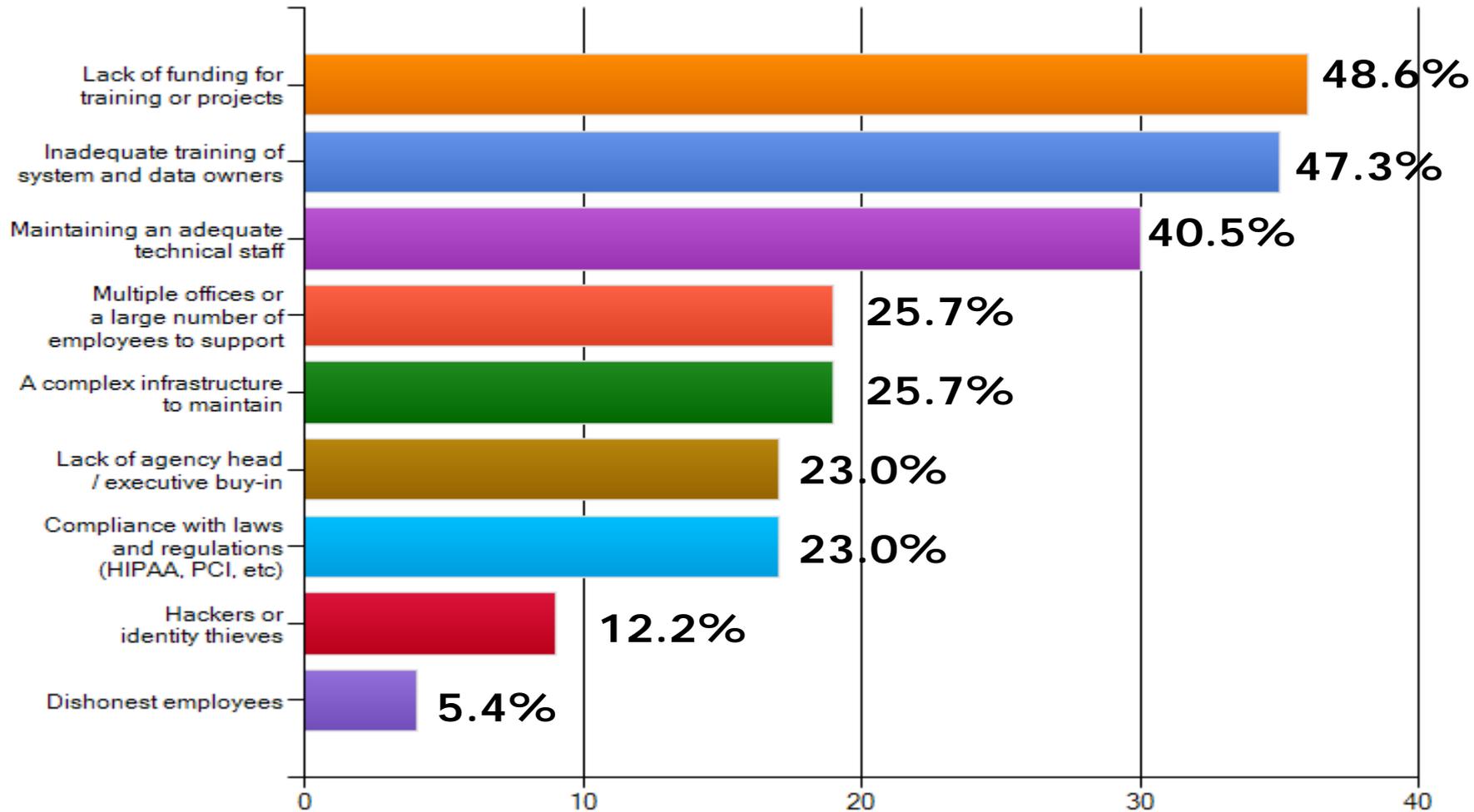


From your perspective, is your agency adequately resourced in terms of budget, personnel and skill sets for information security?





What challenges do you feel are the most significant in terms of information security (select up to 3)?





Survey Summary

- A significant % of ISO's report that they:
 - Do not have a professional certification (64%)
 - Do not attend very much annual training:
 - 18.3% = 0 hours per year
 - 36.6% < 10 hours per year
 - 17.1% ~ 10 to 20 hours per year
 - Note: Most professional certifications require a minimum of 40 hours of continuing education per year.



Survey Summary

- When asked if professional certification would benefit themselves or their agency:
 - 56.1 % say yes
 - 43.9% say no

- When asked if their agency had adequate resources for IT Security:
 - 64.6% say no
 - 18.3% are not sure



Survey summary

- When you were asked to tell us “what other challenges” do you face as an ISO, the most repeated comments focused on:
 - A lack of resources or staff
 - And
 - A lack of training or skills



Survey summary

- The survey gave us a better understanding of where we currently are in terms of agency security management in the Commonwealth.
- It also gave us some ideas of where we have some gaps in where we would like to be and some areas in which we can work towards improving.



CSRM Initiative

- CSRM feels that IT security education, training and workforce development are key components in making Commonwealth systems secure.
- IT security certification is one of the ways in which many organizations try to assure that their IT security personnel are equipped with baseline competency and have the knowledge and skills needed to effectively promote and elevate the level of IT security in the entity.



CSRM Initiative

- CSRM believes that the role of the ISO in the COV is an important & complex position that involves a highly significant percentage of an individual's job duties.
- For this reason, ISOs need to make a commitment to continuing education and professional development.
- IT security certification can help improve the overall security of the COV by assuring that the people who manage & promote security in each agency have the appropriate baseline knowledge & skills.



CSRM Initiative

- CSRM recognizes and commends a large number of ISO's who already hold a professional IT security certification, such as CISSP, CISM, SANS or others.
- CSRM also encourages all ISO's who do not currently have a professional IT security certification to obtain one.
- We are actively trying to expand existing educational resources in order to provide affordable professional certification to all COV security personnel.



CSRM Initiative

- In addition to certification training for certain internationally recognized IT security certifications, we are also looking to add affordable technical & role-based security training for all COV security personnel on a number of topics. The training will be developed and provided by an established professional training partner.



ISO Certification

- CSRM also realizes that although there a number of high-quality certifications in the IT security area available, none of them were specifically tailored to address the unique security environment mandated for Commonwealth IT systems.
- We want to provide a framework where ISO's can extend their training and experience to demonstrate their expertise in the specific IT security requirements of the Commonwealth.



ISO Academy

- ISO Academy will be a Knowledge Center based training resource available to all COV personnel.
- Courses will be developed and added to the KC over time. The course material will initially focus on the skills most identified as being needed by you:
 - Security plans
 - Risk assessments
 - BIA development
 - And others
 - COV Policies & Procedures
 - Contingency planning
 - Data sensitivity classification



ISO Certification

- The COV Certification Program will provide two paths that ISO's can take to obtain COV certification:
 - 1. For those who currently have or will soon obtain a professionally recognized IT security certification
 - And
 - 2. For those who currently do not have or do not wish to obtain an IT security certification.

Steps to obtain COV ISO Certification for those who already have a professional security certification:

Possession of recognized professional IT Security Certification	CISSP, CISM, CISA, SANS (others to be determined)
VITA Training	Attend Information Security Orientation training
ISO Academy	Successful completion of at least one course in the KC ISO Academy per year
ISOAG attendance	Attend at least one mandatory ISOAG meeting per year (waived for calendar year 2012)
Continuing Education	Maintain compliance with the continuing educational requirements of the professional IT security certification body

Steps to obtain COV ISO Certification for those who do not have a professional security certification:

VITA Training	Attend Information Security Orientation training
ISO Academy	Successful completion of at least 2 - 3 courses per year in the KC ISO Academy
ISOAG attendance	Attend at least one mandatory ISOAG meeting per year (waived for calendar year 2012)
Continuing Education	Obtain an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to 3 hours each!)



Summary

- We hope that this effort will enable the Commonwealth to assure that we have ISOs that:
 - Are equipped with the skills and knowledge needed to effectively manage an agency's security program,
 - Able to promote security awareness,
 - Able to implement & maintain the proper level of security controls,
 - Can mitigate / report security incidents,
 - And can maintain and enhance an effective working relationship with Commonwealth Security & Risk Management.



- Questions
- Thank You!



Virginia Information Technologies Agency

Upcoming Events





Information Security System Association

ISSA

DATE: Wednesday, June 13, 2012

LOCATION: Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

COST: ISSA Members: \$20 & Non-Members: \$25

SPEAKER: *Peter Coddington, PaRaBaL*

TOPIC: iPhone Security



Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - July **11**, 2012 (2nd Weds. due to holiday)

Topic: PCI Challenges : Andrew Hallberg and Shirley Payne

Family Feud game with Ed Miller

Wednesday - Aug 1, 2012

Topic: FBI – Mobile Devices Overseas

ISOAG will be held the 1st Wednesday of each month in 2012



IS Orientation Sessions

Tuesday - Aug 7, 2012 1:00 – 3:30p
(CESC)

Email CommonwealthSecurity@VITA.virginia.gov if you are interested in attending.

IS Orientation also available via webinar!



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

June 6, 2012



NORTHROP GRUMMAN

ADJOURN

