**Acknowledgments**

**ISACA wishes to recognize:**

**Board of Directors**
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA, KPMG LLP, UK, International President  
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President  
Tony Hayes, FCPA, Queensland Government, Australia, Vice President  
Avinash Kadam, CISA, CISM, CBCP, CISSP, GCIH, GSEC, Miel e-Security Pvt. Ltd., India, Vice President  
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President  
Jose Angel Peña Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President  
Robert E. Stroud, CA Inc., USA, Vice President  
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP, USA, Vice President  
Frank Yam, CISA, FHKCS, FHKIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice President  
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President  
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President  
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, Director  
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director

**Security Management Committee**
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, Chair  
Juan Manuel Aceves Mercenario, CISM, CISA, CISSP, Cerberian, Mexico  
Kent E. Anderson, CISM, Network Risk Management LLC, USA  
Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc. and Osaka University, Japan  
Yves Le Roux, CISA, CA Inc., France  
Mark Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA  
Vernon Richard Poole, CISM, CGEIT, Sapphire, UK  
Jo Stewart-Rattray, CISA, CISM, Vectra Corporation, Australia  
Rolf von Roessing, CISA, CISM, CISSP, FBCI, KPMG Germany, Germany

**CISM Certification Board**
Evelyn Susana Anton, CISA, CISK, UTE, Venezuela, Chair  
Garry James Barnes, CISA, CISM, CIA, Commonwealth Bank of Australia, Australia  
Allan Neville Boardman, CISA, CISM, CA, CISSP, JP Morgan Chase, UK  
John Randolph Caraway, CISM, CISSP, JP Morgan Chase, USA  
James A. Crawford, Jr., CISM, CISSP, MSIA, Marine Forces Reserve, USA  
Ramses Gallego, CISM, CISSP, SCPM, SurfControl, Spain  
Kyeong-Hee Oh, CISA, CISK, CISSP, Fullbitssoft, Korea  
Hitoshi Ota, CISA, CISM, CIA, Mizuho Corporate Bank Ltd., Japan  
Smita Dilip Totade, Ph.D., CISA, CISM, FEI, National Insurance Academy, India
Table of Contents

CISM Career Growth ................................................................................................................................. 5

Education .................................................................................................................................................. 5
  Figure 1—Highest Level of Education Completed ............................................................................... 5
  Figure 2—Importance of Education in Specific Categories ................................................................. 6

Certification .............................................................................................................................................. 6
  Figure 3—Importance of Professional Certification in Specific Categories ........................................ 7

Career Progression ................................................................................................................................. 7
  Figure 4—Reasons for Beginning a Career in Information Security ................................................... 8
  Figure 5—Comparisons of Primary Position Roles at Current and Prior Jobs ................................. 8
  Figure 6—Ten Most Common Activities Performed by CISM in Current and Prior Positions ........... 10
  Figure 7—Next Career Step for CISM .............................................................................................. 10

Conclusions ........................................................................................................................................... 10

Other Publications ................................................................................................................................. 11
CISM Career Growth

The Certified Information Security Manager® (CISM®) designation, offered by ISACA®, is growing rapidly. Only five years old, it has already been earned by more than 9,000 professionals worldwide since its inception. Recognition and respect are also growing for this sought-after certification. In fact, while other certifications seem to be decreasing in value, CISM is generating increased regard and professionals holding the certification are able to command high salaries.

In Certification Magazine’s 2007 Salary Survey, CISM comes in as the second-highest paid IT certification, at an average of US $115,072 annually. This is especially interesting when compared to the fact that in the same survey, security, which was the highest paid discipline in 2006, fell to fourth place in 2007—from an average salary of US $93,500 to US $87,890. At US $115,072, CISM is clearly being recognized as an asset among business leaders.1

What makes CISM stand out? The CISM certification identifies a seasoned professional who has experience in areas such as information security governance, risk management, information security program management, information security management and incident response.

This experience enables professionals to build and manage effective information security programs and also to demonstrate the value of information security to executive management. CISMs are experiencing tremendous career growth while acquiring responsibility for issues that demonstrate value to the business.

In November 2007, ISACA conducted a survey of CISMs worldwide. In total, 1,426 CISMs from 83 countries participated in the study. Survey respondents represented more than 20 different industries, with the highest populations in:
  • Banking and financial services (26.6 percent)
  • Consulting (23.75 percent)
  • Technology (12.5 percent)
  • Government (12 percent)
  • Healthcare (4.2 percent)

The purpose of the survey was to examine how those in information security management positions have arrived at their current position, what types of activities CISMs are accountable for, and where they see themselves in the future. Major areas of the study include education, certification and career progression.

Education

In general, CISMs are a highly educated group, as shown in figure 1. At least a bachelor’s degree is held by 86.9 percent of respondents, while 49.1 percent hold an advanced degree. While educational specialization varies considerably, the top three educational areas of focus include computer science (24.6 percent), business/management (23.8 percent) and information security/information assurance (17.8 percent).
Education is highly valued: 78 percent of polled CISM1s claimed that their education has been important in their career.

Education factors into many aspects of a career, as shown in figure 2. When asked what importance education has played in different situations, many respondents felt that education was important for obtaining a job in information security (72.1 percent) and also for promotability within a career (77.8 percent). The most important factor, however, seems to be related to performance within the specialization of information security, as 84.1 percent of respondents stated that education was important because it added value to their role in security.

The value of education, as seen by the CISM1s who participated in this study, attests to the need for a strong alignment between business and security management. Almost 42 percent of CISM1s have pursued a degree in business or within the specialized area of information security or assurance. An increase in both undergraduate and graduate programs with a specialization in information security has demonstrated the importance of information security as its own discipline. Information security requires a unique curriculum to prepare students to face core business requirements as well as issues such as technology and regulation.

Certification

IT certifications are proliferating. Professional and technical certification bodies address different levels within the information security profession.

With so many certification choices available to information security professionals, it is interesting to observe which ones they value. The certification section of the ISACA questionnaire was separated into two sections: certifications were labeled as either a “professional certification” or a “technical certification.” Survey respondents reported differing opinions regarding certifications and their value.

For the most part, “professional” certifications are vendor-neutral, testing management and business skills. These certifications demand that candidates not only pass an exam, but also demonstrate substantial relevant professional experience. A few examples of certifications considered “professional” for this study included the CISM and: Certified Information Systems Auditor™ (CISA®) by ISACA, Certified Internal Auditor (CIA) by The Institute of Internal Auditors, Certified Information Systems Security Professional (CISSP) by (ISC)2 and Certified Protection Professional (CPP) by ASIS International.

Technical certifications are often vendor-specific, more technical in nature, and may offer multiple certification levels demonstrating different degrees of experience. Examples of certifications considered “technical” for this study included: Cisco Certified Security Professional (CCSP), Microsoft Certified Systems Engineer (MCSE-Security), Security+ (CompTIA Security+) and Global Information Assurance Certification (SANS/GIAC).

---

Figure 2—Importance of Education in Specific Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adds Value to Role</td>
<td>84.1%</td>
</tr>
<tr>
<td>Promotability in Career</td>
<td>77.8%</td>
</tr>
<tr>
<td>Obtain Job in Information Security</td>
<td>72.1%</td>
</tr>
</tbody>
</table>

1. CISM: Certified Information Systems Manager
A large number of information security managers reported holding professional certifications in addition to CISM. In fact, 45 percent have the CISSP certification and 43.1 percent have attained CISA certification.

In addition to professional certifications, 24.8 percent of survey respondents also hold technical certifications. Of those, 18.6 percent maintain a current TruSecure Internet Security Certified Associate (TISCA), 15.7 percent hold an MCSE-Security, and 12.2 percent have CERT’s Certified Computer Security Incident Handler Certification (CSIH) designation.

When asked about the overall importance of a professional certification (see Figure 3), 81.7 percent of respondents agreed that certification is important overall. Specifically, 92.3 percent indicated that their professional certifications are important to demonstrate competency in their job, 88.7 percent felt they are important in gaining professional recognition, 82.9 percent pointed to their importance in gaining recognition from peers and 77 percent felt they are important in qualifying for a new position. Also, 61.9 percent of respondents indicated that they intend to pursue additional professional certifications.

These numbers changed significantly when respondents reported the importance of technical certifications. When holders of technical certifications were asked how they felt about the overall importance of their technical certification, only 38 percent said that having the certification was important.

Among technical certification holders, only 47.9 percent felt that having the certification was important to help demonstrate professional competency, 42 percent felt that the certification had helped them to prepare for a career in information security, 39.3 percent felt that the certification had been important in helping to gain professional recognition and 36.7 percent felt as though their technical certification would be important in helping to qualify for a new position. Only 15.6 percent of technical certification holders reported that they will pursue additional technical certifications.

**Career Progression**

As diverse as certification and educational circumstances are, so too have been the ways CISMs have progressed within their careers (see Figure 4).

When asked how they became involved in information security, CISMs had a variety of answers. The largest number of respondents, 25.5 percent, said that they chose information security simply because it was an interesting field; 14.3 percent cited that they became involved with information security because their role in IT emerged as a distinct professional competency; 8.6 percent indicated that they entered the field because of a job opportunity; 7.3 percent noted that they entered information security without preplanning a specific career; and 7.1 percent stated that the market demand and business needs pushed them into security.
To see how CISM roles and responsibilities have evolved, it is necessary to compare positions and responsibilities of CISM in their current position and the one immediately prior. This provides a view into the evolving job responsibilities, titles and reporting structures that CISM have experienced within their career progression (see Figure 5).

Clear career growth is shown when position roles are considered. For example, when CISM were asked about their prior position, only 7 percent claimed a position in information security executive management. This position description was not even one of the top five positions. When asked about their current position description, information security executive management placed second, with 14.4 percent of respondents describing themselves as such. Information security provides career progression and CISM are moving into top leadership positions.

In addition, 33.5 percent of CISM described their current role as that of information security management, which is an increase of 10.9 percent from their previous role. Combining the two top positions, the survey shows that 47.9 percent of respondents categorized their current role as either information security executive management or information security management. Only 29.6 percent of respondents categorized their previous role the same way. CISM are experiencing significant opportunities for career advancement.

A decrease is seen in the number of CISM who described their current role as an information security technical position. At 6.5 percent, this description did not place in the top five descriptions for the current position, but was third—with 10.7 percent—in previous role descriptions. The role of information security manager is evolving to be one that focuses on the application of technology to solve business problems rather than being a purely technical specialization.

Figure 4—Reasons for Beginning a Career in Information Security

Figure 5—Comparisons of Primary Position Roles at Current and Prior Jobs
In addition, 43.6 percent of respondents stated that in their prior position they reported to senior management or to a director; 30.6 percent said that they reported directly to executive management and 18.7 percent reported that they answered to someone at a manager level. Reporting at higher levels in the organization, CISM are expected to bring value and to participate in more strategic business-related activities.

When the reporting lines of current roles are considered, growth is reflected once again: 40.6 percent of CISM polled stated that they now report directly to executive management and 41.4 percent report to senior management or a director. Only 13 percent of respondents are currently reporting to someone at a manager level.

When these statistics are examined, it is clearly evident that CISM are experiencing career growth. Whether it is moving up higher in management or into management for the first time, a consistent pattern of advancement is demonstrated.

As can be imagined with such a shift in job roles, responsibilities have changed as well (see figure 6 for the top 10 functions for which CISM claimed responsibility in their current and prior roles).

The ISACA survey compared the activities for which CISM are currently responsible with those they performed in their prior role. The responses revealed that CISM are experiencing a significant widening in the breadth of their responsibilities as well as a change in the type of responsibilities.

In prior positions, survey respondents reported that they had responsibility for technology-focused functions such as data security, network security, disaster recovery, and system and application security. The majority of respondents did not report being accountable for functions that are traditionally business-focused.

However, the functions for which CISM are responsible in their current role are quite different. CISM reported that they are now responsible for more business-related functions such as risk management. For example, when polled on prior job responsibilities, only 54.8 percent of respondents answered that they had responsibility for the risk management function. In their current position, 76.6 percent do. Security program management is also increasingly a responsibility of CISM, from 49.0 percent in their previous role to 74.0 percent in their current one.

Regulatory compliance, at 44.7 percent, failed to break into the 10 most frequently performed activities in prior positions. It was the fifth most frequently cited responsibility in current positions, with 63.4 percent of respondents claiming ownership of this function. This is an indication that protection functions such as compliance and risk management have become increasingly important as business drivers and are receiving more attention from the boardroom.

As noted previously, many of the information security managers who participated in this study had responsibility for technology-driven functions, such as network security, in their prior positions. Their current positions reflect little growth in functions that deal mainly with technology.

Network security was among the most frequently performed activities (third) in prior jobs, with 53.5 percent of respondents holding responsibility for the function. In current jobs, it increased to 57.3 percent. It dropped, however, to the eighth position among most-performed activities. Telecommunications security also increased, but only slightly, from 22.7 percent to 24.7 percent.

It appears that the role of the information security manager is evolving. When comparing responsibilities held by CISM in their current and prior positions, the functions that are gaining momentum are those more significantly aligned with business needs and priorities. The information security management role is becoming increasingly focused on business enablement rather than on technology.
When asked what their next career step was, 27.1 percent of respondents answered that they intend to step into a chief information security officer (CISO) role.

The growth pattern among CISM s is very clear. CISM s have been able to move up into management ranks and have also acquired more responsibilities, particularly those with a business focus. Given that CISM s are experiencing significant career growth, it is not surprising that survey respondents still intend to strive for further expansion in their career.

When asked about their next career step, 40.6 percent of respondents (27.1 + 13.5) answered that they intend to step into an executive management role. Of those, 27.1 percent see themselves in a chief information security officer (CISO) role (see figure 7).

Conclusions

Information security is an evolving profession. In the past, technology dictated security; now business is the main driver.

CISM s have grown in their careers and continue to acquire more responsibility for functions that are closely aligned with business. Regulatory compliance, which did not make the 10 most frequent activities that security managers were responsible for in their prior positions, registered as the fifth most frequent in current roles. In addition, CISM s are taking responsibility for functions such as risk management, governance and architecture. These are the areas that will help to demonstrate the value that information security provides to the enterprise.
Other Publications

Many publications issued by ITGI and ISACA contain detailed assessment questionnaires and work programs. For further information, visit www.isaca.org/bookstore or e-mail bookstore@isaca.org.

Security
- Cybercrime: Incident Response and Digital Forensics, 2005
- Information Security Harmonisation—Classification of Global Guidance, 2005
- Managing Enterprise Information Integrity: Security, Control and Audit Issues, 2004
- Security Awareness: Best Practices to Serve Your Enterprise, 2005
- Stepping Through the InfoSec Program, 2007

Assurance
- Stepping Through the IS Audit, 2nd Edition, 2004

Specific Environments:
- Electronic and Digital Signatures: A Global Status Report, 2002
- Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment, 2004
- Linux: Security, Audit and Control Features, 2005
- Oracle® Database Security, Audit and Control Features, 2004
- OS/390—z/OS: Security, Control and Audit Features, 2003

ERP Series

IT Governance
- IT Governance Global Status Report—2008

COBIT® and Related Publications:
- COBIT® 4.1, 2007
- IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance, 2007

COBIT Mapping Series

IT Governance Domain Practices and Competencies

Val IT