FUTURE-PROOFING A CAREER IN CYBERSECURITY

IS ARTIFICIAL INTELLIGENCE A CAREER PATH FOR YOU?

EFFECTIVE STRATEGIES FOR CREATING AND MAINTAINING A DIVERSE AND INCLUSIVE IT AUDIT TEAM

FUTURE-PROOFING

YOUR CAREER
INTRODUCING COBIT 2019

The globally recognized COBIT® Framework has been updated with new information and guidance—COBIT 2019 extends its leading role in implementing and ensuring effective enterprise governance of information and technology (EGIT).

COBIT 2019 is an evolution of COBIT 5, so this newly revised governance framework contains everything you love about COBIT 5, plus many new exciting features and focus areas.

COBIT 2019 CORE PUBLICATIONS

For more information on COBIT 2019, its publications and guidance, and new training opportunities, go to www.isaca.org/COBITv6
Learn from top compliance and ethics professionals and build your professional network at this conference dedicated to learning about the challenges facing the global compliance & ethics community. This is the place to find out about the latest solutions to your compliance and ethics issues, including anti-corruption, data protection, and risk management.

EuropeanComplianceEthicsInstitute.org

Questions? beckie.smith@corporatecompliance.org
The ISACA® Journal seeks to enhance the proficiency and competitive advantage of its international readership by providing managerial and technical guidance from experienced global authors. The Journal’s noncommercial, peer-reviewed articles focus on topics critical to professionals involved in IT audit, governance, security and assurance.

Do not miss out on the Journal’s online-exclusive content. With new content weekly through feature articles and blogs, the Journal is more than a static print publication. Use your unique member login credentials to access these articles at www.isaca.org/journal.

**Online Features**

The following is a sample of the upcoming features planned for November and December

**The Age of PowerShell**
Ignacio Marambio Catán, CISA, CRISC, CISM, CISSP, Security+

**Automation, Governance and Security in a Software-Defined World**
Julio Pontes, CISM, BS7799 LA, CCSK, CISSP

**Launching a Value-Based Analytics and RPA Program**
Chris Sanders, CISA, COBIT 5 Foundation

---

**Features**

3 Information Security Matters: How We Can Succeed
Steven J. Ross, CISA, CISSP, AFBCI, MBCP

6 IS Audit Basics: Affect What Is Next Now
Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt, and Martin Cullen, CISA, CGEIT, CRISC, COBIT Foundation, COBIT Assessor and Implementer, ISO 27001 LA

10 The Practical Aspect: Why Worry About IoT?
Vasant Raval, DBA, CISA, ACMA, and Ranjit D. Thaker, CISA, MCSI

14 The Network
Glory Ninsiima, CISA, CompTIA Security+, ISO 27005, ISO 31000, ITIL Foundation, PRINCE2 Foundation

16 Future-Proofing a Career in Cybersecurity
Mike Saurbaugh, CRISC, CISM, CISSP, MSIA

20 Is Artificial Intelligence a Career Path for You?
Larry G. Wlosinski, CISA, CRISC, CISM, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL V3, PMP

28 Effective Strategies for Creating and Maintaining a Diverse and Inclusive IT Audit Team
Julie Balderas, Asim Fareeduddin, CISA, CISM, CIPP, CPA, Femi Richards, CCEP, CIPP, Ruwel Sarmad and Jack Wall

37 Growing a Cybersecurity Career
Philip Casesa

41 Defining the Chief Digital Officer Using COBIT 5
João Catarino, Isabel Rosa, Ph.D., and Miguel Mira da Silva, Ph.D.

49 A Heightened Sense of Awareness
Wade Cassels, CISA, CFE, CIA, CRMA, Kevin Alvero, CFE, and Randy Pierson, CISA

PLUS

54 Tools: Skill Acquisition in a Rapidly Evolving Workplace
Robin Lyons, CISA, CIA

56 Crossword Puzzle
Myles Mellor

57 CPE Quiz

59 Standards, Guidelines, Tools and Techniques

S1-S4 ISACA Bookstore Supplement

---

Read more from these Journal authors...

Journal authors are now blogging at www.isaca.org/journal/blog. Visit the ISACA Journal blog, Practically Speaking, to gain practical knowledge from colleagues and to participate in the growing ISACA® community.
How We Can Succeed

In my last article, I excoriated the information security community, of which I am a card-carrying member, about the state of security today. Moreover, I stated my opinion that the underlying architecture of distributed systems, the most commonly implemented since the late 1980s, is incapable of supporting a tolerable level of security. Thus, we have suffered through viruses, worms, denial-of-service (DoS) attacks, botnets and cyberattacks for more than a generation.¹

A New Era

Just as the distributed model displaced the centralized (i.e., mainframe) one, I now believe that we are on the threshold of a new era, that of a multi-modal, utility, cloud-based, commercial, Software as a Service (SaaS) (choose any two terms at your pleasure) architecture. Both ownership and geography differentiate the “utility SaaS” architecture from those that went before.² In the centralized era, ownership of data and software rested within the organization, which kept both of them in one big room. In the distributed era, i.e., today, the organization still owns the data and software, but these may or may not all be in the same place. In the cloud-based multi-modal environment that is now arriving, the organization retains ownership of the data, but not the software, nor does it house the computing.

Many core business functions are routinely being performed or supported in the cloud and have been for several years. For example, organizations increasingly turn to commercial services for customer relationship management (CRM), payroll, human resources (HR), order entry, accounting, inventory, supply chain and many other automated business functions. The economics of using cloud-based services just make sense. No single organization can afford to have staffs of specialists to develop and maintain software for each function in the way that a vendor specializing in that function can do. Recognition of the total cost of ownership (TCO) drives organizations toward the cloud. The question of build vs. buy is passé; today, it makes sense to rent.

Security in the Commercial SaaS Environment

The same point, overwhelmingly, applies to information security. No organization that I am aware of has a team of security professionals for each application. But, for cloud-based service

Steven J. Ross, CISA, CISSP, AFBCI, MBCP

Is executive principal of Risk Masters International LLC. Ross has been writing one of the Journal’s most popular columns since 1998. He can be reached at stross@riskmastersintl.com.
vendors, this is a commercial necessity. The incentives for a vendor’s security include not just financial, legal, reputational and regulatory risk—as though those were not enough—but existential risk as well. The inability of a cloud-based software vendor to implement and maintain security over its products and services will likely put it out of business.

Zero Trust

In fairness, using a variety of cloud-based services does not an architecture make. And well-secured applications do not by themselves make the entire environment safe. More is required before we can say that we have improved significantly on the shortcomings of the distributed era.

In several previous articles in this space, I have referred to the Zero Trust Model. It is not exactly a standard, although it has the imprimatur of the US National Institute of Standards and Technology (NIST), in a publication called “Developing a Framework to Improve Critical Infrastructure Cybersecurity.” In a very brief synopsis, in the Zero Trust Model, all networks—and, by extension, the information systems on the network—are untrusted. All resources are accessed securely regardless of location. Access to resources is based on a least-privilege strategy and access controls are strictly enforced. All network traffic is inspected and logged.

The architecture that can be built on the Zero Trust Model is based on a segmented network with all security-related controls established at a single point of entry and transfer. These controls constitute a unified threat management gateway. In practice, this gateway is a “next-generation firewall” (NGFW), sold by many equipment manufacturers. By itself, NGFWs are necessary but insufficient for effective security. A secure architecture must be based on rigorous network segmentation such that a user authorized for one domain cannot traverse the network without returning to the access control mechanism. That mechanism must include what some have called “next-generation access” (NGA), with advanced functionality such as correlation of users and uses, machine learning to identify anomalies, and technical integration with the security features at the network level. The complete implementation of the Zero Trust Model is being referred to as the Zero Trust Extended Ecosystem (ZTX).

Getting to Success

This is all wonderful in theory, but organizations are not about to re-architect their entire IT environment around an enhanced security. But they are migrating to multi-modal environments as a pathway that can lead to ZTX, if information security professionals exert their influence now. As increasing numbers of applications are being used as cloud-based services, organizations are realizing that they are dealing with too many clouds. They are seeking a “cloud of clouds,” one cloud to control them all. And that is where the Zero Trust Model can be implemented.

Let me paint a word picture of what I believe is the future of information security. All uses of information are defined in domains, and all users are associated with one or more domains. All security controls are embedded in a central control point (the cloud of clouds). An authenticated user can proceed to a domain and do what he or she is authorized to do and nothing more. To do anything else, the user must return to the control point and be reauthenticated and reauthorized. All of these accesses are recorded and analyzed at the control point and any anomalies are reported.
The roles of information security professionals will be transformed from passive policy making and active implementation to that of vendor management and security monitoring. One very positive sign that this transformation has begun is that many information security professionals are already involved in, and occasionally arbiters of, SaaS acquisition decisions.

I am not so naïve as to think that all this wonderfulness will arrive due to a sudden enlightenment in the executive ranks. To be sure, some of it will occur because of the persuasiveness of chief information security officers (CISOs). I think a lot more will happen because organizations will back into intolerable situations with uncontrolled acquisition and use of services, with only zTX as a way out. And some will happen because, at long last, the zeitgeist is ready and willing to pay for secure computing. I am convinced that this is the way in which we information security professionals will succeed.

And then, when that happens, I will not be able to author this column because there will be nothing to write about. Nah. There will always be new challenges. Keep your seat belts fastened; it could be a bumpy flight.

Endnotes

2 I realize that the dates of these eras are approximations. Mainframes did not disappear in 1985; in fact, they are not gone today. And the cloud did not suddenly spring into existence in 2015. The fact that boundaries are fuzzy does not mean that they do not exist. A highly unscientific search for the first mention of “the cloud” came up with “The Self-Governing Internet: Coordination by Design,” by S. Gillett and Mitchell Kapor (yes, the Mitch Kapor of Lotus) in January 1996 (http://cits.mit.edu/papers/CCSWP197/CCSWP197.html).
6 Ibid., p. 5
To celebrate its 15th birthday, LinkedIn asked its members to share what they wanted to be when they were 15. Now, I do not know about you, but an auditor was not on my list, nor did I, or any of my friends, take turns at playing auditor and auditee! And yet, we became IT auditors. How did this happen? I certainly do not believe (at least, not entirely) that life is what happens to you when you are busy making other plans. We are where we are because of a series of conscious decisions. The question now becomes how do we make conscious decisions to create, grow, improve and add value to our lives, our enterprises and the profession?

At EuroCACS 2016 in Dublin, Ireland, the closing keynote speech was given by futurist Mark Stevenson. It was described by a colleague sitting next to me as the best talk he had ever heard. The talk centered on eight principles that Stevenson derived from traveling and working with successful optimists. That colleague, Martin Cullen, went on to read Stevenson’s book, so I tasked him to collaborate with me in reviewing the principles and their relevance to IT auditors.

Have an Unashamed Optimism of Ambition

Stevenson recommends not feeling embarrassed to say that things can be better. People should have no qualms about imagining an improved world and advocating for it, no matter how much derision they may receive at the hands of the cynical.

This is not about the next promotion. This is about seeing that things in audit are not as they should be and they could be better. Those who believe this is the case should advocate for it in their enterprise. And those who are not sure how things can be better can reach out to their peers in the ISACA Online Forums.

Engage in Projects That Are Bigger Than You

Philosopher Daniel Dennett says that an occupational hazard of his profession is being asked, “What is happiness?” The best definition he has come up with is to “find something more important than you are and dedicate your life to it.”

There are many issues directly related to the adoption of new and innovative technologies in the world today. Examples range from the erosion of privacy to the lack of female representation in the industry. ISACA is a leading advocate in these areas with the introduction of its privacy principles, several documents around the EU General Data Protection Regulation (GDPR) and its SheLeadsTech program. Auditors who are
passionate about these topics can do something about them by getting involved.

ISACA is always looking for volunteers, and any ISACA employee will agree that it is the volunteers who make the organization what it is.

Ideas Are for Sharing, Not Protecting

Every new idea is, as Matt Ridley suggests, the result of the joining together of two other ideas. Pragmatic optimists happily let their ideas meet and mingle with others.

Back in my very first column in this space, I asked why, when we live in a world where it is very much a viable option to run a business using open-source software, we, as an ISACA community, do not develop open-source audit/assurance programs? To me, this is an idea waiting to meet someone else’s idea. Would it be possible, for example, to use GitHub, Slack or ISACA’s Online Forums? I am not certain, but I believe it needs others’ ideas to help push it over the line.

I am also sure that everyone reading this column has ideas of their own. I would like to hear them. Only together can we truly move the IT audit profession forward.

We have all made mistakes during our careers and in audits. The key is to learn from them and not be afraid to try again. After every audit, each auditor should take some time to sit back and consider how it went. What went well? What mistakes were made? How could it be done better the next time? Audit-specific items should be documented and added to the audit file as there is every chance the auditor may be requested to audit this item again.

You Are Defined by What You Do, Not by What You Intend to Do

Pragmatic optimists are not interested in what others might do if they had more time or if their manager was more understanding or if they were the manager or if it was next week. People are what they do. That is it. Get on with it.

LinkedIn is full of conversations about the unimportance of certifications when compared to experience and, yes, there is no doubt that experience really counts. However, if people are defined by what they do, does not the fact that they have put in the effort to attain that certification say something about them? Lack of time is no excuse. Make time! Those who believe they have all the certifications they need can translate, write or review items. Exam Item Development Working Groups are composed based on geographical representation. Those who participate learn so much.
Be an Engineer

Engineers do not build bridges from a left-wing or right-wing perspective. They build bridges from an evidence-based perspective and, over time, bridge building gets better. Politicians make their decisions from an ideological perspective and, (in the opinion of many), over time, politics gets worse. No one should ignore politics, but those who choose engineering will do more.23

This is key. Audit recommendations should be based on agreed criteria24 and have the required evidence to back them up. If the evidence was obtained in an interview, it should be documented and the auditee sent a copy or a draft report produced in which the auditee is asked to confirm the auditor’s understanding.

As for politics, the auditor should remain sufficiently neutral to maintain independence while still being aware of how decisions are reached. That is, the auditor must understand who has the ability to make, ignore and overturn decisions; whether these are taken unilaterally or by consensus; and the degree to which they represent a compromise. Without such knowledge, the recommendations in the audit report may not be followed and the audit function could, consequentially, be discredited.25

Be Prepared to Lose Nine Battles Out of 10

No one can win them all, but anyone is likely to win one battle out of 10. In “round two,” the auditor may win one battle out of nine and, by round three, one out of eight. By that time, the auditor will have created enough of a shift for the rest to follow. Those who worry about losing nine out of 10 will likely never enter the fray. It is useful to concentrate on winning the one. Overnight success is for the movies.26

This is about winning the war, not the battle. All IT auditors have been here. They have identified a significant issue and, being conscientious and aware of the politics, they have reported the finding to management early only to be told at the exit interview that there is no issue or the issue has been resolved and should no longer be in the audit report.

My advice? If there is no compelling reason not to and it is possible to confirm that the risk has been addressed, the item should be removed. The auditor has done his or her job. The job is to help mitigate risk, not to have findings. Not only that, it has been accepted that the auditor’s recommended course of action was the correct one; this will work in his or her favor the next time a similar issue is found in another application. Furthermore, the auditor is building a relationship of trust with the auditee. This will be helpful the next time there is a finding that cannot be removed.

Kick Out Cynicism

Cynicism has become embedded in society and it is often seen as wisdom. Yet there is nothing wise or even likeable about cynicism. For the cynic, everything is just a little too hard to imagine or do. As such, cynicism is both a recipe and an excuse for laziness. Auditors should have no time for it.27

It can be very easy to become cynical and even have a sense of futility when working as an IT auditor. This is especially the case when finding the same issues across different applications and nothing ever seems to change. I urge IT auditors to avoid this and try to think differently. Could the applications be audited horizontally?28 Could the issues be tackled from another angle?29 Remember culture, ethics and behavior of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.30 Peers in ISACA’s Online Forums may be a good source of help in this area.

Conclusion

At the end of the day, if there is one guiding principle that encapsulates all these principles, it is, “Judge your worth not by what you own, but by what you create.”31 ISACA is the vehicle that allows IT auditors to learn and create. When I was 15, I was torn between IT and journalism. ISACA has enabled...
me to do both. Along the way, I feel I have created, I have grown and I have improved. This, in turn, has brought value to my enterprise. As it approaches its 50th anniversary, ISACA can allow anyone reading this article to do more, too. Members can affect what is next, now. Pragmatic optimism tells us that the future is still a game worth playing and all players can make a difference.32

Endnotes

1 Lennon, J.; Beautiful Boy (Darling Boy), USA, 1980
5 ISACA® Online Forums, Audit and Assurance, https://engage.isaca.org/communities/onlineforums
6 Encyclopaedia Britannica, Daniel C. Dennett, https://www.britannica.com/biography/Daniel-C-Dennett
7 Op cit Stevenson 2012
10 ISACA, SheLeadsTech, https://shelleadstech.isaca.org/
11 ISACA, Volunteer Opportunities, https://engage.isaca.org/volunteeropportunities/about
13 Op cit Stevenson 2012
15 GitHub, https://github.com/
16 Slack, http://slack.com/
17 ISACA Online Forums, https://engage.isaca.org/communities/onlineforums
19 Op cit Stevenson 2012
20 Ibid.
21 Op cit ISACA, Volunteer Opportunities
23 Op cit Stevenson 2012
24 “Criteria” is defined as the standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter. ISACA, “ITAF: Information Technology Assurance Framework,” www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Assurance-and-Assurance/Pages/ObjectivesScopeandAuthorityofITAudit.aspx
26 Op cit Stevenson 2012
27 Ibid.
30 Op cit ISACA, Audit and Assurance
31 Op cit Stevenson 2012
32 Ibid.
A recent post on a neighborhood blog read:

Our camera picked up a suspicious young male, approximately 17-24 years old, who approached the house, looked to the right of home, into the side door window, front door lock and into the camera before walking away quickly. Cannot be certain about his intentions, but wanted to make the neighborhood aware. My husband left message with the police department.

So, the old door locks are not the same as today’s smart locks with sensors, cameras an Internet connectivity. These locks not only prevent physical intrusion, but also do reconnaissance, record evidence along with a time stamp, and alert the owner and others charged with security responsibilities to act promptly.

The Internet of Things (IoT) refers to physical objects that have embedded network and computing elements and communicate with other objects over a network. It is a network of items—each embedded with sensors—that are connected to the Internet. These objects or devices possess at least two attributes: Each has a unique identifier and the ability to share data and interact remotely over a network without human intervention. These devices communicate over the network via wireless protocols such as Bluetooth; they are not dumb, but rather “smart.” For example, the motion sensors embedded in the application (app) that supports the camera at the front door generated all images and alerted the device owner to the risk of an uninvited visitor.

The concept of IoT has become more real—more available—with the presence of the Internet combined with smart devices of recent origin. Over a relatively short period of time, smart devices have become smarter—that is, faster, with greater capacity to work with data, more processing capability and at a lower cost. And yet, what seemed like a wave of transformation enabled by IoT has lost some steam lately.

And yet, there is considerable optimism in what is anticipated in the world of IoT. According to a collaborative report on IoT in logistics, compared to 15 billion connected things in 2015, there will be 50 billion things connected to the Internet by 2020. However, this represents only 3 percent of all connectable things, which continue to grow in number and sophistication over time. The proliferation of embedded sensor technology, wearables and apps has already caused incredible change in just a few short years. It can be concluded that “we are just beginning to connect everything unconnected.”

Vasant Raval, DBA, CISA, ACMA
Is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include information security and corporate governance. He can be reached at vraval@creighton.edu.

Ranjit D. Thaker, CISA, MCSM
Is the chief information officer for a leading time-critical, same-day air and ground transportation service provider. He has been in this role for more than 10 years. He has served in IT leadership positions in the specialty logistics industry for more than 25 years. He can be reached at ranjit.thaker@gmail.com.
Early evidence of the revival of IoT rests in the arrival of 5G. Citing MOBI, a Wall Street Journal article suggests that 5G could connect a trillion devices in the next decade.

There are two distinct domains in which IoT has flourished. First, early adoption of the concept emerged in the industrial or manufacturing settings, where the supply chain was made more efficient or effective, perhaps even addressing issues of safety in the workplace. The following examples of such applications are drawn from the transportation logistics industry:

- **Tracking**—Most used for parcel or delivery service providers to track shipments and keep customers up to date on location of their shipment/estimated time of delivery
- **Environmental parameter tracking**—Used for sensitive cargo (e.g., specimens, organs, pharmaceuticals) to monitor temperature, humidity, speed, shock, etc.
- **Vehicle maintenance and driver behavior**—Used to optimize fuel efficiency, reduce breakdowns and monitor driver behavior (e.g., speeding, frequent breaking, lane violations)
- **Inventory management and operational optimization within warehouses**
- **Data analytics**—Analytics based on data collected from IoT devices and their use in improved decision support

Industrial IoT (IIoT) was a logical extension internally within the organization. The insights generated from the supply chain are harnessed into IoT apps developed and embedded into the supply chain support platform. Information security and privacy issues in IIoT are more easily controlled because the applications are within the boundaries of the organization, and devices and software are probably screened prior to acquisition. And their scope is tightly perimeterized, although anchored on the Internet.

A later development pushed IoT applications into the consumer arena, which can be called Consumer IoT (CIoT). Because it involves reaching out to customers who may have varying security environments and perhaps a variety of different devices among them, achieving reasonable goals on privacy and security fronts may be a challenge.

The relative newness of integrating consumers into the IoT ecosystem adds a formidable dimension to the implementation of CIoT. It is challenging to understand the IoT footprint and control dimensions on each class of IoT devices. Also, IoT devices and technology integrate with several private and public network segments with a combination of privileged and open access; hence, a traditional third-party risk management (TPRM) approach to control devices and software needs an IoT technology-specific control domain to mitigate additional risk. The problem with these IoT devices is that they are made by consumer electronics companies. Unfortunately, consumer electronics products change often, adding to the risk scenarios. And even these organizations are themselves new to this level of computing and, therefore, vulnerable to making rookie errors in their firmware code.

Perhaps there are IoT applications that cut across IIoT and CIoT. However, from an information security viewpoint, it is easier to see the challenges if such applications are identified using this binary classification. The former is mature, better controlled, better known to the organization and limited to the internal network(s). The latter is new, introduces more devices from more vendors (likely from the consumer electronics industry), and connects the external customer to the internal world or internal employee to the outside world. Clearly, the IIoT ecosystem lands more comfort on the privacy and security front. CIoT is early in its development and, while popular and exciting to end users, needs more groundwork before an organization ventures into CIoT applications.

**Essential Questions**

Here are some essential questions that need to be addressed, among other things, to ensure that IoT is introduced to the organization with care and due
diligence. Some of these questions apply equally to just about any IT introduction, but are certainly worth repeating because of the fundamental nature of the question of technology adoption:

• Do you have a business case for the use of IoT?
Technology is an enabler of value creation; its use just for the sake of using it could be valueless. It is important to ask first, “Does the organization have the potential to create value through the adoption of IoT?” The answer to this question may change over time; therefore, it is important to revisit the question at appropriate intervals. Leaving the question buried in the past could hurt the organization’s competitiveness.

• Do you have a policy on the deployment of IoT?
Do you have other policies that support the IoT initiative? Once it is determined that IoT adoption could potentially help create value, the development and use of a policy toward adoption of the technology should be considered. Without such a policy, a controlled and intentional introduction of IoT that meets the organization’s policy criteria is not possible. Just like the rules in configuring a firewall, the first rule is to not allow anything in, then progressively modifying the rule to embrace what is desired.

• What appear to be the weakest links in defense-in-depth of the IoT ecosystem? Network privileges and access vulnerabilities are the most significant. Where to draw the line in terms of allowing a network to access IoT applications is crucial to stemming any compromise of security. The security management should be quite discrete about what is essential to provide and what is a luxury, causing more risk than benefits to the organization. Another weak link in the CIoT environment is smart consumer electronics and the difficulty of tracking their ability to provide things acceptable under the organization’s policy. The extension of TPRM to the IoT ecosystem is easy to visualize but difficult to implement due to its diversity, vastness and constantly changing characteristics of the devices produced. It is doubtful if one can rely on the device makers to provide adequate security in the product features. Finally, the consumers who get connected to the IoT may not be aware of vulnerabilities that their use of the application would engender, and this could consciously or unconsciously enable a cyber compromise.

• How do you limit the seemingly pervasive IoT networks? First, a business case for each implementation must be made and, if this is done successfully, the minimum number of networks that should be allowed access to the IoT applications should be determined. Second, restricting scope and limiting risk is greatly affected by how well the perimeter of the network carrying the IoT traffic is controlled and how strong the access privileges to the network are. Sound security practices driven by a sound policy framework provide essential big steps toward secured IoT networks. Finally, user education is important, especially in the CIoT environments where users may be remote to the risk; their awareness and cautious behavior are soft, but important, components of IoT security.

• How do you keep up with the continued development of the field (i.e., device, device makers, software, firmware)? Should the organization trust smart devices its employees bring to work? As the Strava incident has taught us, any device capable of running software could become problematic if that software is transmitting intelligence about the enterprise’s network. Employees could use their smartphones to run a seemingly innocent Internet speed test, for example, and end up sharing details about the internal network architecture that should be kept private. While service level agreements (SLAs) could help gain some assurance that devices engaged in IoT are secure, it would be difficult to implement a similar mechanism on the CIoT side, for the consumer electronics device makers are too diverse and do not necessarily focus on serving organizations in a one-to-one relationship as the third parties. Besides, continuity of electronic device makers or their products may be uncertain.

There are few technology fronts where, upon adoption, one can choose to rest without periodic evaluation. It is necessary for organizations to constantly monitor changes in the domain space to determine if any action needs to be taken at their end. What might have been launched as a potential value could quickly dissipate or could result in greater risk than anticipated. To continue to leverage the organization’s strategic and operational excellence, it is necessary to continuously be on the lookout for the edge of the innovation in IoT.
In as much as technology is an enabler, not taking advantage of it in a timely manner could, in fact, disable the enterprise. Today, it is not a choice to allow a technology to pass by without the organization conducting a thorough review regarding its potential role in value creation for the organization. A technology may get hot at times and cold during other times; however, keeping an eye on its edge is an important first step toward continuing to leverage the technology. Not all technologies may fit a larger, or any, role in an enterprise at any given time. However, scanning the environment to reflect on where it is today and what it can do for the enterprise is an opportunity that should not be sacrificed. That is why business and IT leadership should worry about IoT.

Endnotes
4. Ibid., p. 26
8. Op cit Jones
Q: How do you think the role of IT auditor is changing or has changed?
A: In the past, the role of the IT auditor was to assess the technical environment and report on the control weaknesses. Today, the IT auditor is taking on an advisory role to management on IT-related issues. The IT auditor needs to be able to translate technical information into operations language that the business can understand and from which it can derive value. Management needs assurance that it is deriving value from IT investments, that the suggestions being made by the IT department are strategically driven and will deliver as promised and that the security posture of the organization is strong. It is the role of the IT auditor to review the governance of IT, IT risk and investment, and give feedback to management in the form of recommendations. The IT auditor needs to look forward internally and externally and identify issues that could affect business performance, assess the control environment against these and advise management on the best way to avert future risk. Technology changes at a rapid pace and IT auditors need to adapt and think innovatively about how the organization can improve its control environment to guard against evolving threats. As the world moves toward artificial intelligence (AI), the role of the IT auditor leans into data analysis and forensics. The IT auditor also must evaluate risk from the perspective of achieving the organization’s strategic objectives.

Q: What leadership skills do you feel are critical to be successful in the technology fields?
A: Patience and the ability to explain and elaborate the value of what practitioners are delivering, especially to a nontech-savvy audience. Soft skills go beyond any knowledge that one may have. Practitioners must also be competent and firm without being excessively aggressive, as this may overshadow or distract from a well-intentioned message.

Q: What is the best way for someone to develop those skills?
A: Develop and harness emotional intelligence. Take up opportunities to lead that are not work related to help prepare for leadership roles. Get a mentor and request feedback from trusted colleagues. One should know their strengths and capitalize on them, for there lies one’s ability to shine. Being competitive and comparing oneself with others only breeds frustration. Know what you are good at and do it. The rest falls in place.

Q: What advice do you have for IT audit professionals as they plan their career paths and look at the future of IT auditing?
A: It is important to network. Use social media to advance your career and put yourself out there. Facebook, Twitter and LinkedIn are great places to learn more about what is going on in the technology field, get to know the buzz in the profession, understand the latest trends and learn how other professionals are conducting themselves. Great communicators capture an audience and easily get buy in from board members and management. Polish your communication and interpersonal skills for these go beyond technical knowledge. Find a mentor or make friends with someone you admire in the field and seek their guidance.

Glory Ninsiima, CISA, CompTIA Security+, ISO 27005, ISO 31000, ITIL Foundation, PRINCE2 Foundation
Is a certified risk manager and IT auditor with eight years of experience in information systems management and IT auditing, mainly in the banking industry. Currently, she is a senior IT auditor with the central Bank of Uganda where she participated in the implementation of IT systems that facilitated the transition from manual processing to automation of all government and nongovernment payments processed by the Central Bank of Uganda. Ninsiima serves as secretary of the ISACA® Kampala (Uganda) Chapter and also as the representative of the African region on ISACA’s International Chapter Liaison Working Group. She is also a member of the Institute of Internal Auditors.
by asking them specific questions about their experience and advice.

Q: What do you think are the most effective ways to address the lack of women in the technology workspace?

A: The number of women who pursue computer science at the university level is typically lower than males and it drops as the students conclude university and choose career paths. This is not helped by the fact that there is a decline in the number of women pursuing science or computer-related courses. These facts make it difficult to have women role models in this industry.

Programs such as ISACA’s SheLeadsTech are a great way to increase the representation of women in technology and encourage taking up leadership roles in this field. They give a sense of identity and security to the women in the field, those intending to join, those exiting and the technology industry at large.

Earning certifications that will make one recognized at the international level goes a long way and gives one a competitive advantage to climb the career ladder. Also, organizations should consider having favorable maternity leave policies and gender balance recruitment programs as part of their organizational culture.

Women need to promote themselves and female colleagues in their work environments. Correcting the gender imbalance in the technology field is not an issue that will be solved overnight. It is a work in progress that calls for the input of organizations, women in the field, those intending to join, those exiting and the technology industry at large.

Q: What has been your biggest workplace or career challenge and how did you face it?

A: When I joined the audit profession, I soon found out that internal auditors are the least favorite people in an organization. I had to develop thick skin and realize that the work I do as an IS auditor adds value to the business, improves operations and helps the business see the value of a stronger control environment through implementation of recommended changes. All of that proved encouraging. As the years have progressed, I have found it to be a rewarding profession because one gets to know enterprise operations in its entirety and, therefore, has an edge over the rest in managing operations or during an interview. An auditor can easily work in any field they have audited.

1 What is the biggest security challenge that will be faced in 2019?
Data leakage will continue to be the biggest security challenge faced as digitalization increases every day.

2 What are your three goals for 2019?
• Take a long overdue vacation
• Change the work environment
• Spend more time with family

3 What is your favorite blog?
ISACA’s Nexus, Bright Talk and Gartner.
I also enjoy health-related blogs.

4 What is on your desk right now?
The organization I work for enforces a clear desk policy, so currently there is a cup of warm water, a glass of passionfruit juice, a notebook to keep track of today’s assignments and a desktop computer on which I am typing this.

5 Who are you following on Twitter?
I mostly follow cyber-related tweets and ISACA international news.

6 How has social media impacted you professionally?
Social media has helped increase my professional network and keep abreast of the latest news in technology.

7 What is your number-one piece of advice for other IT audit professionals, especially women?
Be bold. Do not wait for the perfect moment; that moment is now. Use the resources at your disposal to get to the next level.

8 What do you do when you are not at work?
I enjoy reading inspirational stories, fine dining and spending time with family and friends.
Help wanted! Millions of security professionals needed to help fill critical roles required to protect the world’s infrastructure, data and people—apply now!

Security professionals are in high demand, but the challenge is that there are not enough qualified employees to fill open enterprise requisitions. For confirmation, it is worth taking a look at ISACA’s report State of Cybersecurity 2018. Part 1 of the report outlines workforce development and mentions that 59 percent of the respondents to the survey upon which the report is based have open, unfilled security positions. Years of costly incidents and breaches have led to chief executive officers (CEOs) worrying about security threats. PricewaterhouseCoopers 2018 report Threats: What Keeps CEOs Up at Night Differs by Region highlights that executives are concerned about cybersecurity threats—a concern that was ranked number 10 in 2017, but has risen to number four in 2018. Cybersecurity is now a top executive topic and one that has the board of directors paying attention, too.

Though there is seemingly no end in sight for enterprise anxiety over security issues, there is no guarantee employees will have perpetual job security and be immune to changes in the industry that disrupt human capital. Security professionals need to evolve and enhance their careers to better position themselves for continued employment because technology and automation will be a priority for security leaders playing catch-up to the adversary.

Whether candidates are new to the security field or have some tenure, it is imperative that they not rest on their laurels and keep advancing the career skills that employers are seeking.

### Technical Skills—Taking Initiative and Learning Something New

Security practitioners have plenty of opportunity to learn new skills, in many cases at low to no cost. Employers will likely allocate some budget to obtaining new skills, but, regardless, practitioners need to invest in themselves and assume the employer will not. Technology moves too quickly to sit back and get comfortable.

Employees should be dabbling in new technology to at least understand the basics. Years ago, building a lab would have required expensive hardware and licenses. Today, there is a plethora of opportunity to build a lab in the cloud at minimal cost. This is a fantastic way to build something, break something, build it back again and then share the experience with others. It is a great story to tell. There is significant value in explaining this in a technical interview or, as an experienced hire, being able to convey to a potential team the ability to “walk the talk.” In many cases, this may be enough to land the next internal or external position.
The list of new technologies continues to grow, but there are a few that stand out in the short term, despite the list’s ongoing expansion. Following are a few growing areas where practitioners can and should devote some time to help ensure that they are in a better position to land that next role:

- Python
- PowerShell
- Amazon Web Services (AWS)
- Microsoft Azure
- Docker
- Analysis and incident response
- Application security
- Kubernetes
- Threat intelligence
- Threat hunting
- Forensics
- Malware analysis
- Penetration testing
- Data science fundamentals

While this is not an exhaustive list, Coursera, edX, LinkedIn, Udacity and Udemy offer various technology courses for free or at low cost. Also, Microsoft offers training on Azure, and Amazon offers training on AWS.

Ultimately, technical skills will more than likely win the job for the candidate. This can be hard, especially for experienced candidates who have progressed up the management ranks. It is all the more reason for managers who are not doing the day-to-day hands-on work to do their best to keep their skill set up as much as possible.

**Soft Skills Matter**

Conversely, employees who have fewer years of experience, but aspire to a higher-level position should be working on attributes that will set them apart. Soft skills do matter. It is very easy to overlook soft skills in the security and technology field.

Soft skills are personal attributes that support interaction with other people. It is much different from the solitude that often comes with technology work and extended computer time with the screen and keyboard providing bidirectional communication.

It is no secret that businesses rely on technology, making cybersecurity a key area of focus for businesses eager to protect systems and data. Soft skills are required to obtain buy-in from the business. Many technologists excel in technology due to requirements for system security, uptime and functionality, and may not have essential soft skills.

What soft skills and personal attributes are influential in career growth? Many of these are no surprise, but they are sometimes given less focus:

- Communication (written, verbal)
- Team orientation
- Organization
- Project management skills
- Service orientation
- Business finance comprehension
- Business acumen
- Emotional intelligence
- Empathy
- Listening
- Personality
- Negotiation

Enjoying this article?

- Read State of Cybersecurity 2018—Part 1: Workforce Development
  www.isaca.org/state-of-cybersecurity-2018

When embarking on a course, it may become apparent quickly that it is not the right path. It is okay to fail fast. Practitioners’ curiosity and interest in trying something new, especially in the security field, should be an expectation and something employers seek. Determining that the technology is not interesting or it is too much of a struggle to grasp the basics is fine, but it is important to move on and try something else as opposed to remaining comfortable.
Soft skills translate into professionalism, too. In other words, career advancement often depends on professional growth and dropping bad habits that hold people back. Being someone who others want to work with can be a significant career advantage. Managers can always train skill, but ridding employees of a bad attitude is a completely different challenge and one that many are not willing to fight long term. It goes without saying in information security, but for the sake of full inclusion, it is important to stress the need to be true and genuine and hold a high degree of integrity.

The Importance of a Professional Network

Building a strong professional network is essential. Employees who spend too much time isolated from others in their industry are likely to find it difficult to pivot to the next organization when they want to make a change. This is not to say loyalty and dedication to one's organization is a negative, but time does need to be made for connecting with others.

Some may find this rather obvious and are well on their way to establishing a strong professional network. Surprisingly, though, it is easy for some to stay within their comfort zone and not engage with others. The challenge is that when these individuals are seeking their next position, they may have trouble finding a role they desire. Many positions are not posted externally and sometimes, before they are even posted, up-and-coming opportunities may be known to peers. Those who are connected may stand a better chance of getting an earlier opportunity to demonstrate that they are the better candidate.

Obviously, social networking is a great place to get started. Professionals do not have to be the most acclaimed user of Twitter or LinkedIn, but they are advised to have some sort of presence (at least on LinkedIn). In addition, conferences are a great place to meet new people and start to forge new relationships. It may be uncomfortable for those who are not overly social, but there is a need to start making connections one by one. There is no shortage of low- to no-cost conferences to meet new people in the local area. Many global events can be attended online.

Conferences need speakers. Consideration should be given to submitting to the call for papers (CFP). Speaking at conferences is a great way to improve one's personal brand. Done well, it is a way to start being identified as a leader in a particular discipline. However, speakers must beware because the security industry will scrutinize the content, so speakers need to be prepared to deliver highly informative presentations.

Give Time to Help Others

Those who have learned a lot should share their knowledge. What does this do for a career? For starters, it helps promote a personal brand and recognition in the industry. In addition, it increases education on the topic among technical and nontechnical people. This is a common outcome of conference talks and individual blog posts. The security industry thrives when practitioners and managers share what they have learned, both good and bad, in their day-to-day activities.

It is great when security knowledge reaches a technical audience, but what about nontechnical people? The average person who has a smartphone and/or a computer uses most of the same applications as the rest of the world when it comes to office work and social media. Volunteering some time to help educate nontechnical people on how to better secure their data and the systems they use can go a long way toward expanding one's technical reach in the world. It also helps practitioners work on communication skills. Acronyms do not work well with laymen or the business. This is a chance to hone in on enhancing communication skills to get the point across.

This activity makes for a great conversation with current and potential future employers. It is a blend of so many useful traits that employers seek: technical prowess, soft skills, contributions to the profession and initiative, to name a few. Furthermore, it is not uncommon for employers to have a volunteer program initiative for the workforce in which professionals can contribute and help increase knowledge, skills and abilities among those involved.

For more experienced professionals, mentoring junior employees can be a rewarding experience. Granted, a lot of this will be done within the organization itself, but it is not to say that it cannot be done outside the corporate environment, too. If someone reaches out and shows genuine interest in learning from experience, it is a good time to lend a hand. At the same time, mentoring should not be overly draining, so managing the time allocated is important.

Additional Options and Resources

Certifications have been sought by practitioners for years and still hold a place for many in the industry.
Their value varies, based generally on the enterprise hiring. If an organization requires certifications, then there is value in holding one or more. Some organizations do not care and are more interested in job skills than in whether candidates have initials after their name. But, in general, certifications carry merit.

For newer employees in the field, they are certainly worth looking into and obtaining. Credentials from CompTIA, ISACA®, (ISC)² and SANS, along with vendor-specific certifications, offer the opportunity to indicate to employers that a certain level of mastery has been achieved. Additionally, and this goes for experienced employees, it also shows some dedication to the field and career. After all, unless an employer is requiring a certification, a lot of this is based on initiative and exemplifies dedication to and passion for one’s career path.

A respected personal development resource, regardless of the employee’s career focus, is StrengthsFinder,¹¹ which helps people identify their strengths vs. calling attention to weaknesses. The idea is to continually capitalize on strengths to be more successful. Too often, weaknesses are the focus, which can drag people down. However, by leveraging strengths, people tend to excel and are happier in the process.

Those who wish to remain informed on what is going on in the industry job market should check out CyberSeek,¹² which is a culmination of career path information for employers, employees, educators and students.

The National Initiative for Cybersecurity Education (NICE),¹³ offered by the US National Institute of Standards and Technology (NIST), focuses on education, training and workforce development. The framework on which the initiative is based¹⁴ outlines knowledge, skills and abilities that are needed to perform tasks in a role.

Conclusion

Careers are what people make of them. There are no guarantees. It is in a person’s best interest to continue to evolve and not sit back and wait for something to happen. The security field needs all kinds of people with diverse backgrounds and experiences. As mentioned earlier, technical skills tend to capture the most attention, but there is a need for well-rounded individuals. When faced with a choice, it is preferable to err on the side of learning more on security technology, but still putting some effort into soft skills as time allows.

The job market continues to look promising for quite some time, but it is unlikely to last forever. In the meantime, putting in the extra effort to learn a new technology, enhance soft skills and build a professional network while giving back in the process is likely to result in the phrase, “You are hired!”

“THE SECURITY FIELD NEEDS ALL KINDS OF PEOPLE WITH DIVERSE BACKGROUNDS AND EXPERIENCES.”

Endnotes

3 Coursera, www.coursera.org/
4 edX, www.edx.org/
5 LinkedIn, www.linkedin.com/
6 Udacity, www.udacity.com/
7 Udemy, www.udemy.com/
11 Rath, T.; Discover Your CliftonStrengths, Gallup Press, USA, 2007
12 Cyber Seek, www.cyberseek.org/
Is the world changing too fast? Can society continue to do the best it can? The population is currently more than 7.6 billion. The amount of data accumulated is predicted to exceed 44 zettabytes (or 44 trillion gigabytes) by 2020, with a growth rate of 1.7 megabytes per second for every human being. The number and types of data-gathering devices, sensors and mechanisms are growing to feed the need to obtain, process and manage the data. So how can an individual help?

What has been happening in industries where artificial intelligence (AI) is used is examined herein. Also reviewed are the AI software industry requirements, the skill sets and job requirements for AI, the marketplace and job options available for entering the field of AI, and the earning potential.

AI Definition
First, it is important to know the definition of AI. There are many, including:

- “The study and design of intelligent agents’ where an intelligent agent is a system that perceives its environment and takes actions which maximizes its chances of success.”
- “Simply put, artificial intelligence is a sub-field of computer science. Its goal is to enable the development of computers that are able to do things normally done by people—in particular, things associated with people acting intelligently.”
- “The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.”
- “The ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.”

These sample definitions show how diverse and evolved AI is. Here, the definition from a worldly and job requirement perspective (and not necessarily robotics) is examined.

AI Usage
AI can be used for many purposes, including answering questions, searching documents, performing language translations, improving marketing efforts, monitoring information security and being a home assistant. Figure 1 contains examples currently in place.

These examples show that the AI industry started some time ago. Some readers may be thinking that it left them behind. Part of the reason for this...
<table>
<thead>
<tr>
<th>Usage</th>
<th>Example</th>
</tr>
</thead>
</table>
| **Answer questions (i.e., chatbots, virtual agents)**                | - A North Carolina (USA) government office uses a chatbot to free up help center operators.  
- New York City (New York, USA) built a system to answer questions and complaints about city services.  
- Surrey, British Columbia (Canada) developed an application (app) to address 65 percent of questions that may be on city websites.  
- An instant messaging application has been programmed to provide text and emoji responses.  
- Retail chatbots can recommend outfits (H&M), give beauty tips (Sephora) and provide direct ordering (e.g., Dominos, 1-800-Flowers).  
- TV remote controls can retrieve information about requested programming (e.g., types of programs or particular programs or movies).  
- PennyCat, a Facebook Messenger bot, allows users to find coupons (which aids in coupon use).  
- Conversational bots from China (e.g., Xiao) provide interactions in the financial sector (banks, securities, insurance) and accounting.  
- Healthbots walk users through symptoms to diagnose the likelihood of a particular illness.  
- Some organizations use AI to provide personalized fund management advice. |
| **Search documents**                                                 | - A chatbot lawyer app helps refugees determine which application to use.  
- One US state government is using AI to help citizens search documents on more than 1 million pages while saving tens of thousands of US dollars that would have otherwise been spent in upgrades.  
- The legal profession is using scanned legal documents to find related case law.  
- Turnitin searches massive databases of reference material and foreign language sources to check for plagiarism.  
- Amazon searches through its inventory to provide recommendations based on relevance to previous user purchases or searches.  
- Based on searches of existing media, some apps can recognize faces in photographs and newfeeds. |
| **Route requests**                                                   | - An insurance company uses a chatbot to answer questions about its plan and payments and provides directions to the nearest office.  
- A telecommunications provider uses AI to search documents to aid call center agents in responding to inquiries. |
| **Perform translations**                                            | - The Pyeong Chang Winter Olympics used AI real-time software to respond to questions in 14 languages.  
- Some apps perform text-to-speech (TTS) and speech-to-text (STT) to power voice-based search. |
| **Draft documents**                                                  | - Japan’s Ministry for Economy, Trade and Industry has a system to help parliament member offices respond to citizen questions by drafting answers.  
- Newsrooms use AI to mine data, create text for data sets and write stories. |
| **Audit**                                                            | - Auditors can analyze large amounts of data to detect anomalies (e.g., fraud).  
- Auditors can use AI to search documents and databases to extract relevant information for review. |
| **Information security**                                            | - Software vendors are developing AI tools that can monitor trends and activities on the network and perform data forensics.  
- AI can provide security intelligence solutions for detecting, monitoring and managing information security threats and risk factors.  
- AI is used to perform behavioral fingerprinting to detect and defend websites. |
| **Mobile phone assistant**                                          | - Siri and Google Now perform Internet searches, set reminders and integrate with users’ calendars.  
- Alexa creates to-do lists, orders items online, sets reminders and answers questions via Internet searches.  
- Echo Dot smart speakers integrate Alexa to answer natural language questions, play music, order pizza, hail an Uber car and integrate smart home devices.  
- Smartphones can retrieve directions (e.g., global positioning satellite [GPS]) and traffic reports.  
- Google Maps uses Waze to obtain and report traffic conditions. |
feeling may be that AI is technical in nature and requires expertise from people who are analytically inclined. Those in the auditing and fraud detection fields can see that the world has changed/evolved from reviewing and cross-checking simple lists and databases and searching large amounts of data to data accumulation, information extraction and personal assistance (at home, at work, in transit and elsewhere). AI can be used as a tool to search for problems, crimes, anomalies and potential solutions in the mountains of data that are continually growing. So, AI may be a possible new tool for many people’s work belts. What follows is an overview of the technology and insight into the required skills for this new era of discovery.

### AI Technology

AI technology can mean many things, but it can be broken down into the following:

- **Machine learning (ML)**—“Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it (to) learn for themselves.”

- **Deep learning (DL)**—“Deep Learning is a subfield of machine learning concerned with algorithms that are designed to mimic the way the human brain learns to identify patterns.”

<table>
<thead>
<tr>
<th>Usage</th>
<th>Example</th>
</tr>
</thead>
</table>
| **Home assistant**         | * Home devices use voice-controlled natural language to interface with consumers.  
* Google Home and Amazon Echo respond to voice commands to play music; answer natural language questions; provide sports, news and finance updates; call Uber; make appointments; and issue reminders.  
* Jarvis connects home devices into one network. It learns music preferences and can recognize friends at the door and let them in. |
| **Driverless transportation** | * Postauto in Switzerland has driverless buses.  
* Alphabet Inc., Uber Technologies, General Motors and Tesla Inc. have all developed driverless cars. |
| **Marketing**              | * Marketers can compile customer interests based on social media activities to group people with similar interests.  
* Regression techniques can be used to predict numerical product values.  
* Computer vision for branded object recognition can provide data from video analysis.  
* AI marketing apps can read emails, open and analyze attachments, perform data entry for template reports, and track social media triggers to stay ahead of the curve.  
* Data analytical solutions like Qlik can centralize data sources and generate dashboards and reports for marketing teams.  
* Apps can generate photorealistic images from sketches. |
| **Detect crimes**          | * ShotSpotter uses smart city infrastructure to triangulate the location of a gunshot. It is now used in more than 90 cities.  
* Hikvision:  
  – Scans for license plates on cars  
  – Runs facial recognition to search for potential criminals and missing people  
  – Automatically detects suspicious anomalies like unattended bags in crowded venues  
* Hashtag mining of social media can help law enforcement officers become better informed. |
| **Prevent future crimes**  | * PredPol claims to be able to predict where future crimes will likely happen by using historical data and observing where recent crimes took place.  
* CloudWalk detects suspicious changes in behavior or unusual movements (e.g., pickpocket, indicator of a future crime).  
* Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) makes decisions about pretrial release and whether to give an individual parole. |
| **Obtain information**     | * New visual sensors (e.g., cameras, stored videos) can obtain, gather and search new and captured data for information requested (e.g., a person, vehicle). |
| **Create new things**      | * AI-programmed computers can produce original writing, imagery, music, industrial designs and even AI software. |
inspired by the structure and function of the brain called artificial neural networks.9

- **Natural language processing (NLP)**—“Natural language processing (NLP) is a branch of artificial intelligence that helps computers understand, interpret and manipulate human language. NLP draws from many disciplines, including computer science and computational linguistics, in its pursuit to fill the gap between human communication and computer understanding.”10

- **Virtual agents (chatbots or virtual assistants)**—“A Virtual Agent is a computer generated, animated, artificial intelligence virtual character...that serves as an online customer service representative. It leads an intelligent conversation with users, responds to their questions and performs adequate non-verbal behavior.”11

- **Speech recognition**—The capability of an electronic device to understand spoken words

- **Hardware with AI**—Contains custom/specialized AI computer chips

- **Decision management**—Rules-based automation (if-then logic)

**Figure 2** describes the capabilities of AI technology and includes organizations that support this field of expertise.12, 13

**Requirements**

Those who want to enter this career field need to learn some things. Here is a short list of prerequisites for learning AI:

- Strong grasp of mathematics (i.e., linear algebra, calculus, probability and statistics, multivariate calculus, graph theory, matrices, and optimization methods)

- Strong experience with programming languages (e.g., C, C++, Java, Python, R) and frameworks (e.g., TensorFlow and scikit-learn)

<table>
<thead>
<tr>
<th>Figure 2—AI Technology Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technology</strong></td>
</tr>
<tr>
<td>Machine learning</td>
</tr>
<tr>
<td>Deep learning platforms</td>
</tr>
<tr>
<td>Natural language processing</td>
</tr>
<tr>
<td>Natural language generation</td>
</tr>
<tr>
<td>Virtual agents and chatbots</td>
</tr>
<tr>
<td>Speech recognition</td>
</tr>
<tr>
<td>Hardware with integrated AI</td>
</tr>
<tr>
<td>Decision management</td>
</tr>
</tbody>
</table>
Understanding of the basic concept of automation and how it relates to computer science

- Understanding of AI principles and techniques
- Ability to write algorithms for finding patterns and learning
- Strong data analytics skills
- Strong will to learn machine learning languages

One may notice that accounting, auditing and conducting assessments are not on the list. This is because AI is a different profession, but one that can be used to aid accountants and auditors. There are many possibilities for AI to assist those who are confronted with large amounts of data to analyze. AI can make a job in the audit field easier by taking over the tedious work of looking for fraud, crime and supporting information. Auditors should reach out to the AI staff in their organization to identify investigative tools and techniques to help them in their job.

Training and Education

AI training is widely available. The training can be obtained online or formally:

- **Free online**—Udacity and Coursera are two companies among many that provide online training.
- **College and university education**—AI training is available in 26 countries and there are more than 25 colleges that provide training.
- **AI certification**—Even certification in AI is available. Microsoft, Columbia University (New York, New York, USA), Stanford University (California, USA) and Global Machine Learning provide certifications in AI.

The availability of so many avenues to learn AI has not only helped this field of expertise to grow, but has also led society to an era of better focused and available healthcare, quicker service (e.g., chatbots), better crime-fighting tools (e.g., traffic surveillance, fraud detection), and a better understanding of existing data.

Some of the skills that can be gained from AI training include:

- **Domain knowledge**—Research or business related
- **Visualization**—Seeing the story in the data
- **Data governance**—General oversight, including ethics and security
- **Engineering**—Understanding the hardware, software and storage capabilities available and how to utilize them
- **Management/curation**—Sourcing, cleaning and manipulating the information
- **Analytical approaches (data analytics)**—Applying various levels of precision for the solution
- **Machine learning**—Teaching computers to recognize patterns
- **Probabilities and applied statistics**
- **Algorithms and advanced modeling**
- **Applicable AI-related programming language**
- **Natural language processing**
- **Computer vision**
- **Robotics**

AI Marketplace

With the increase in population and data-gathering comes big data and data analytics. These two topics are propelling the world into a more manageable place and one where unseen information is now visible. The top industries that are using and accelerating the fruits of AI are Internet of Things (IoT) devices, robotics, social media and e-commerce. There are many organizations (some more well known than others) that gather and analyze the data of many diverse areas of interest. Many are listed on the Datamation and Forbes websites, to name only two sources. Areas of new growth include microfinance, social justice and medical diagnosis. These organizations use AI to make their business grow and be more effective. Other AI-vested enterprises and job opportunities can be found by searching the Internet.
Position Descriptions

Here are some sample AI position descriptions that will help in understanding the AI career field. The descriptions, which will vary by organization, include:

- **ML (or software) engineer**—Runs the operations of an ML project and is responsible for managing the infrastructure and data pipelines needed to bring the code to production.

- **AI programmer**—Develops algorithms and operating software that can be used for robots, AI programs or other AI applications.

- **Business intelligence developer**—Responsibilities include designing, developing and maintaining business intelligence solutions; crafting and executing queries; and presenting information (e.g., reports and presentations).

- **Research scientist/applied research scientist**—Builds on leads/ideas from data scientists or experiments with new approaches.

- **Data scientist**—Tackles discrete problems using preexisting data to validate models.

- **Research engineer**—“Responsible for performing and analyzing research across various disciplines, working with engineers to conduct complex engineering testing and analyses, designing and implementing new standards, protocols, processes and equipment and providing technical reports and presentations to assist in planning and direction. Research engineers may also be responsible for developing prototypes, as well as researching and developing new technologies and materials for use in the creation or improvement of products and services.”

- **Solutions architect**—Organizes the development effort and is responsible for the project vision/solution and its execution.

- **Senior product manager**—Responsibilities include developing product requirements and road maps; leading product managers and coordinating with engineering, marketing and other teams; and incorporating feedback and input from customers, partners and in-house teams on product strategy and finding ways to expand product market reach.

Salaries

Salaries for people who obtain a master’s degree in AI are high. More than 8,000 AI positions were posted on LinkedIn in May 2018. Figure 3 contains average AI-related salaries for positions described, as obtained from Indeed and Payscale.

Conclusion

It is clear that AI is an established industry. Many organizations are using it, the technology exists, there are many ways to obtain training, and there are professional associations, magazines, competitions and books that support AI.

So, those who are analytical, have an understanding of business, are technically inclined, and love to do...
research and explore data should consider a career in AI. The benefits include a high salary, a challenging career and knowing that one's efforts will help not only one's enterprise, but everyone affected by it.

This information helps illustrate the benefits, not just for individuals, but for the future (e.g., healthcare, human and crop genetics, fraud detection, criminal investigations, forecasting, pharmaceuticals, medical science, teaching, customs monitoring, identity authentication, and space and earth science).

Parents, teachers, speakers or leaders may want to talk to their children, students, audiences and colleagues about what the future can hold for them and how they can make an impact on the future of society.

Endnotes

1 Worldometers, www.worldometers.info/world-population/#pastfuture
13 Op cit Yao
16 Coursera, https://www.coursera.org/courses?languages=en&query=artificial+intelligence
17 Class Central, "Free Online Courses in Artificial Intelligence," https://www.classcentral.com/subject/ai
19 AI International, Universities With AI Programs, www.aiinternational.org/universities.html
22 The Microsoft AI training certification program covers topics such as Python, mathematics, ethics, data analysis, Azure machine learning, computer vision, natural language processing and speech recognition. For more information, see https://academy.microsoft.com/en-us/professional-program/tracks/artificial-intelligence/.


LinkedIn, https://www.linkedin.com/jobs/artificial-intelligence-jobs

Indeed, “Ms in Artificial Intelligence Salaries in the United States,” https://www.indeed.com/salaries/Ms-in-Artificial-Intelligence-Salaries

PayScale, “Average Salary for Skill: Artificial Intelligence (AI),” https://www.payscale.com/research/US/Skill=Artificial_Intelligence_(AI)/Salary

Association for the Advancement of Artificial Intelligence (AAAI), https://www.aaai.org/

European Association for Artificial Intelligence (EurAI), https://www.eurai.org/

AI Societies, www.aiinternational.org/societies.html


ENSURE YOUR ORGANIZATION HAS THE CONTROLS IN PLACE TO HANDLE CYBER THREATS AND REDUCE RISK

Introducing the new ISACA® Cybersecurity Audit Certificate Program. Gain the critical know-how to include cybersecurity in your audit plan, reduce cyber-related risk and put mitigating controls in place. ISACA’s new Cybersecurity Training and Certificate Program provides audit/assurance professionals with the knowledge needed to excel in cybersecurity audits. It provides security professionals with an understanding of the audit process, and IT risk professionals with an understanding of cyber-related risk and mitigating controls.

> Choose from three training options, based on your needs. We offer an online, self-paced course, a virtual instructor-led course or an in-person training workshop.

> Companion Study Guide: This handy guide introduces you to cybersecurity and audit’s role, cybersecurity governance and cybersecurity operations. It includes case studies and appendices offering specific cybersecurity audit guidance, frameworks, controls and testing steps.

> Cybersecurity Audit Certificate Exam Voucher: Once you’ve completed your training, schedule and complete this online, remote-proctored exam at your convenience.

ADVANCE YOUR CAREER TODAY. Learn more at www.isaca.org/cybersecurityaudit
Broadly put, it is widely accepted in today’s corporate world that diverse organizations are preferable to their homogenous counterparts. Empirical research reveals that diversity yields myriad advantages, including increased productivity, enhanced problem-solving and heightened levels of employee engagement, among other benefits.

The value of diversity in the context of IT audit teams is worth discussing and a number of practical strategies for creating and maintaining a diverse and inclusive IT audit team as part of an organization’s overall diversity program are offered.

Many countries are experiencing demographic shifts. For example, by 2055, the United States will not be comprised of a single racial or ethnic majority.¹ Millennials are now the largest generational cohort in the US, having surpassed baby boomers, and they are unapologetically challenging the status quo in the workplace.² Women are the primary wage earners in approximately 40 percent of all households with children.³ Simultaneously, there is an increase in demand for individuals with skill sets in information security. The cybersecurity market is “expected to grow from (US) $75 billion in 2015 to $170 billion by 2020,” which is a threefold increase.⁴ Further, by 2019, the number of information security/cybersecurity job openings is expected to rise to 6 million.⁵ “There are one million unfilled security jobs worldwide,” out of which “more than 209,000” are in the United States.⁶ Unfortunately, there is a shortage of skilled candidates to fill these jobs.

To some, these demographic realities, coupled with the inexorable shifts in the job market toward an information worker-driven economy, are unsettling and rattle long-held notions about the very nature of society. In the alternative view, these seismic shifts can be viewed as evidence that the increasing importance of workplace diversity cannot be denied.

**What Is Diversity?**

Asking 10 people to define “diversity” is likely to generate a wide range of definitions. To some,
“diversity” is defined narrowly in terms of race, gender, age or those attributes that fairly easily lend themselves to visual inspection. To others, their definition may depend on whether the attributes in question are afforded legal protection under federal and/or state laws such as Title VII of the US Civil Rights Act of 1964, the Americans with Disabilities Act, the United Kingdom employment equality law, or the Employment Equality Directive and Racial Equality Directive in the European Union—core antidiscrimination statutes that make it unlawful to discriminate against individuals on the basis of sex, race, national origin, color, religion and physical disabilities. Yet others may choose to adopt a broader, more nuanced view that encompasses an expansive range of characteristics that include the aforementioned differentiators, but also embraces such traits as cognitive style, years of service, education, personality, parental status, geographic location and organizational function. Ideally, a comprehensive definition of “diversity” is a relatively fluid concept that reflects a combination of both external and internal elements (figure 1).

In the corporate world, the manner in which “diversity” is defined is important in establishing the context in which individual differences are recognized and celebrated. Moreover, it is critical for the definition to be broad enough that all employees can visualize themselves within the framework of the definition. For example, if the corporate definition is overly narrow and primarily speaks in terms of “advancing historically underrepresented minorities,” it is conceivable that some white males may feel excluded and undervalued by the organization rather than seeing themselves as key contributors to establishing an engaged and inclusive work environment. Diversity, within the specific context of an IT audit team, might pivot on the desire to embrace team members with different educational and professional backgrounds, not limited to experience in IT alone. Given the shortage of experienced candidates and the strong demand for IT audit skill sets, it is important for hiring managers to think “outside the box” and seek out candidates who may not come from traditional IT backgrounds, from both an educational and a professional experience perspective.

The Benefits of a Diverse IT Audit Team

Broadly stated, diverse teams afford underrepresented groups the ability to connect with their peers and colleagues on a level that is comfortable and inclusive. However, this is not the only driver behind the decision of many organizations to expand the makeup and composition of their organizations. An enterprise could simply be motivated by a desire to maximize the effectiveness of its professionals in pursuit of the organization’s strategic business objectives. For example, having a diverse IT audit team could help an organization achieve a competitive advantage because professionals with varied backgrounds can contribute...
innovative thoughts and ideas and a "variety of solutions on how to achieve a common goal." 8

Strong interpersonal skills are critical attributes for a person to excel in the IT audit arena. For example, within RELX Group, the information security assurance team is composed of IT auditors who not only possess considerable technical knowledge of operating systems, platforms and security controls, but who also feel comfortable interacting with senior business leaders, mentoring students or volunteering in the community. By focusing on leveraging each employee’s unique skills, the productivity and performance of the entire team is enhanced. The experienced employees on the team serve as coaches to the campus hires, which allows them to develop and demonstrate their leadership skills. The junior employees also contribute to the team by bringing in a rich skill set from their various professional backgrounds. For example, a recent new hire with work experience in quality assurance (QA) at a global technology enterprise in India was able to use his prior experience to document the QA controls within the audit work papers and assist his colleagues on any QA-related questions. In addition, a senior IT auditor on the team leveraged his prior experience working for a US senator, where he served as a correspondent, event planner, researcher/writer and manager of large projects. His experience enhanced the team’s ability to multitask efficiently and communicate with stakeholders across different business areas via email, phone and in-person meetings. These examples demonstrate how candidates with diverse professional backgrounds can be an asset for an IT audit organization seeking to achieve a higher level of performance.

---

**Figure 1—Dimensions of Diversity**

- **Primary Dimensions (inner core):** Permanent and beyond an individual's control.
- **Secondary Dimensions (outer core):** Subject to evolution over time, less visible, and disclosure to others is more of a choice.

- **Work Style**
- **Education**
- **Religion**
- **Parental/Family Status**
- **Geographic Location**
- **Veteran’s Status**
- **Communication Style**
- **Socioeconomic Status**
- **Political Persuasion**
- **Job Classification**
- **Physical Ability**
- **Appearance**
- **Sexual Orientation**
- **Age**
- **Race**
- **Gender**
- **Ethnicity**
- **Veteran’s Status**
- **Parental/Family Status**
- **Geographic Location**
- **Communication Style**
- **Socioeconomic Status**
- **Political Persuasion**
- **Job Classification**
- **Physical Ability**
- **Appearance**
- **Sexual Orientation**
- **Age**
- **Race**
- **Gender**
- **Ethnicity**
- **Veteran’s Status**
- **Parental/Family Status**
- **Geographic Location**
- **Communication Style**
A diverse IT audit team can bring together employees with different thought processes and backgrounds. This enables a single scenario or situation to be examined from multiple perspectives so all possible outcomes can be evaluated. When seeking to build or augment an IT audit team, hiring managers should ensure the candidate talent pool has individuals with diverse professional backgrounds. By adhering to a more traditional homogenous candidate pool, a hiring manager may overlook and discount some of the more critical skill sets that are required for an IT auditor. Also, by not contemplating diversity, hiring managers run the risk of creating a team in which employees possess not only similar technical perspectives, but also similar aspirations regarding career progression. In other words, a homogenous IT audit team is likely to engage in similar problem-solving modes of thinking and may heighten the risk of increased employee attrition rates if employees choose to leave the organization after reaching an arbitrary ceiling based on similar goals. The IT audit field has numerous job opportunities for qualified candidates, and there is considerable mobility available for both lateral and vertical career growth. Organizations should challenge their employees to broaden their skill sets by encouraging them to work on special projects outside their comfort zone in addition to their regular assignments so they can continue to develop relevant and transferrable skills. For example, an IT auditor who would usually work on information security control audits can also assist with performing periodic risk assessments to gain more experience in a different, but adjacent, field.

Creativity and Innovation

Viewing diversity through the prism of immigration reveals that the inclusion of skilled immigrants in the workforce results in an appreciable boost to innovation that can be empirically measured. Data from the United States can be used as one example. The US National Bureau of Economic Research finds that an increase of just 1.3 percentage points in the workforce population of immigrant college graduates results in roughly a 20 percent increase in the share of patenting per capita.9 It is common to perceive any influx of skilled immigrants as unassailable evidence of the dearth of native innovation. However, one should proceed cautiously when concluding that this increase in diversity automatically crowds out native-born persons from high-skilled occupations. To the contrary, non-native workers simply buttress and sustain the creativity and growth of organizations and have a positive influence on the global economy.

"By not contemplating diversity, hiring managers run the risk of creating a team in which employees possess not only similar technical perspectives, but also similar aspirations regarding career progression."
the abilities of both men and women (and other available diverse employee resources) to ensure that problem-solving efforts draw from the collective wisdom of the team in a way that leads to the best possible result. Moreover, in the information security context, the Arizona (USA) governor’s office recently sought to leverage the strength of a diverse team to solve complex cybersecurity challenges when it announced the creation of the Arizona Cybersecurity Team (ACT). The team consists of 19 state officials with backgrounds in homeland security, infrastructure, academia, the private sector and more.12

To be sure, innovation is a social process that is amplified when different backgrounds interact. The strength of diversity in its myriad forms is that by harnessing the heterogeneity associated with individual experiences and knowledge, organizations can naturally stimulate the work environment in a manner that fosters innovation.

Expansion of the Talent Pool and Assistance With Recruitment
Global unemployment rates have steadily improved since 2000 and, as a result, the hunt for qualified, available talent is fierce.13 Employers who choose to rely on the same tried-and-true recruitment strategies that were effective when there was a surplus of labor may find themselves unable to fill critical positions. Data breaches have become inevitable over time, and with the “wide skills gap for cybersecurity jobs,”14 there is a dire need to fill these cybersecurity job positions.

It is no revelation that cyberthreats are evolving as quickly as the media through which they act. In recent years, cyberattacks have been launched against both the public and private sectors by a variety of actors. State-sponsored attacks, including Korean ransomware attacks against healthcare providers and Russian meddling in US democratic processes, have occurred. Criminals have penetrated the credit juggernaut Equifax. Social hacktivist groups such as Anonymous have released sensitive information pertaining to prominent government officials and corporate executives. The list goes on, but the point is clear: There are a multitude of faces and intents acting in the threat universe, and those faces are daily becoming more varied. This begs the question: Why would forward-thinking organizations fail to expand their information security and IT audit talent pools to include experiences, backgrounds and cultures that can help them cast a broader net across the array of motives, modes and origins behind these attacks? To this point, former US Deputy Chief Information Security Officer, Mischel Kwon, asserts, “In cybersecurity, I always take the view that our adversaries don’t fit into one demographic, therefore, why should we? When security professionals have a broader lens through which to look at security, we’ll be able to provide better answers and support in protecting our systems.”15

Kwon has also strongly advocated for greater female involvement in the field of cybersecurity. According to an (ISC)² study, women represent nearly 50 percent of IT users, but only 11 percent of the global cybersecurity workforce. Regardless of where the blame may lie for the latter figure, one organization in particular, Girl Scouts of America, has taken action. In a move to get more females involved in cybersecurity, the organization has focused on offering a curriculum and certification to educate young girls about cybercrime, network security and computing basics.16

While it is understandable that employers will continue to focus primarily on the applicable skill sets, education and professional experience of the candidates they are recruiting, it is important not to overlook potential candidates who may emanate from nontraditional educational and/or professional...
backgrounds. For example, it may be natural for a hiring manager to seek out candidates from his or her university or individuals who share similar interests or hobbies. However, this method, if followed consistently, is likely to result in a recruitment strategy that does not add sufficient richness to an organization’s talent pool. A more thoughtful strategy may involve seeking candidates who are a departure from the standard recruit, but who still possess the necessary skills and experience and complement the organization’s culture. In this regard, the US military has been successful in trumpeting the numerous benefits and incentives to organizations that commit to hiring veterans.17

Reduced Turnover
Enterprises have come to understand that an engaged workforce is one in which the employees feel a sense of comfort and belonging. If employees believe the organization values their contribution to the enterprise, they are more likely to be productive and loyal. However, an aesthetically pleasing office or gourmet coffee in the break room may not be sufficient to keep employees wedded to the organization if they feel marginalized and alone. Humans are social beings by nature who tend to associate with others who have similar interests, backgrounds and culture. By working hard to increase the representation of diverse groups through targeted recruiting efforts and, equally important, implementing a diversity retention strategy that contemplates everything from mentorship opportunities to the adequacy of compensation to the reputation of the organization in the community, it is possible to send an unambiguous signal to existing employees that the organization’s commitment to diversity and inclusion is more than mere lip service.

There are various professional organizations that focus on information security, IT governance and IT auditing that could be resources for new employees entering the field of information security. ISACA®, the Institute of Internal Auditors (IIA) and the International Association of Privacy Professionals (IAPP) are a few examples of organizations that lead in their respective fields. Employers should support and encourage their employees to attend training/conferences hosted by such organizations so that those employees can gain cutting-edge industry knowledge and incorporate it into their daily job activities. In addition, attendees can network with other experienced professionals at these events to learn and benefit from their experiences. The organization’s support of employee involvement in professional organizations will make employees feel valued, which will help to increase retention.

Conversely, organizations must be careful to not push employees into closed circles, as it may limit the full capacity of exposure to career growth opportunities. Organizations must instead balance the representation of all employees to avoid creating artificial subcategories that subvert the minority’s and the majority’s contribution to the pool of knowledge. An example is affinity groups and the reality that the many of these efforts are not properly funded and are managed only in the spare time of a willing leader.18 This can lead to well-intentioned, but ineffective, support groups that, if improperly managed, may divert attention away from overall assimilation and toward division and seclusion. Inevitably, the summation of all minorities is evolving to be the majority. However, the responsibility to assimilate should not be placed solely on these “outside groups.” Instead, organizations must push for the “inside groups” to also reach outside their comfort zone and enter the normality of diversification. The key to reducing turnover is not simply recruiting for diversity, but to acknowledge that inclusion is key and reaching out should come about from all sides.

Improved Customer Service
This is an area in which changing demographics will have a major impact. For example, the United States is expected to grow to a population of 417 million by 2060, with undeniable growth in the number of what are now considered minorities. Moreover, by 2060, nearly 20 percent of the country’s population will be born outside the United States.19 If these predictions come to pass, businesses must also adapt to the changing composition of their customer base. Organizations that have staff representatives who can speak a multitude of languages, understand various cultural nuances and mirror the communities in which the business resides will be competitively well positioned to serve, satisfy and retain customers.
Strategies to Build and Retain a Diverse and Inclusive IT Audit Team

Successfully building and retaining a diverse and inclusive IT audit team requires tackling the issue as a business problem, not a human resource (HR) issue. Much as an organization would tackle any business issue, such as building a new product or system, it must have a clear, documented go-to-market strategy (with buy-in from the appropriate stakeholders) including the following areas:

- Development of a diversity vision and strategy (tone at the top)
- Targeted recruitment and relationship building
- Investment in employee development and training
- Mentoring
- Use of metrics to track success

A diversity vision and strategy should come from the top down and should be viewed as a business issue owned by the C-suite. To work effectively, the vision and strategy must be adopted at all levels of management. Formal goals should be set, and managers should be held accountable for these goals just as they would for revenue and sales targets. A good starting point for carrying out senior management’s vision is the use of employee resource groups (ERGs), also known as affinity groups. ERGs can partner with different areas of the business, including HR and talent development, to execute a clear strategy to fruition.

The chief complaint from hiring managers is that they would hire someone from a certain background, but they were not presented with any candidates with that background. The easiest solution to this complaint is to target groups and universities where diverse candidates can be identified. Much like a sales pipeline for selling products/services, building these relationships can take time to see the end result. Because of this time-intensive nature, an efficient way to implement such an initiative is to start small. A good start is to build a relationship with an organization or school and ultimately create a repeatable process that can be leveraged across multiple organizations. This is where ERGs can play a key role. It also helps to develop the ERG members’ soft skills, which will play a significant part in on-campus recruiting, guest lecturing/presentations, interviewing candidates and mentoring, to name just a few areas.

Once diverse candidates are hired, it is important to ensure that these employees are retained and feel welcome in the organization. ERGs can be used to assign mentors to candidates to help them navigate the enterprise and its culture. Employees with mentors are less likely to leave the organization and can use the mentor as a support system as they grow through their career. Along with mentorship, it is important to invest in specialized training and development for new employees so they feel constantly challenged and experience growth in the environment.

Organizations should prioritize the professional development of different groups through their internal ERGs.

Predefined steps on the career ladder also assist in retention so that employees have an idea of potential opportunities and specific milestones to achieve those opportunities. Without this infrastructure in place, diverse candidates are more likely to leave the organization, as they may feel that nobody in the organization “looks like them” or cares for their well-being and success.

The old adage “what gets measured, gets done” is as true in the diversity context as it is with any important business-focused initiative. The success or failure of a diversity and inclusion program cannot be effectively quantified without metrics in
place. Goals and objectives should be set up as part of the overall organizational strategy and must be measured at least quarterly, much like financial performance indicators. By assessing metrics on a quarterly basis, senior management will have current information with which to assess the effectiveness of the strategy and make any changes or tweaks along the way. To effect change, these goals and measurements should be part of a manager’s annual performance review.

**Conclusion**

Diversity is more than compliance with laws and rules. It is more than a mere empirical exercise of counting people and assigning them to discrete boxes on a spreadsheet. It is even more than just “doing the right thing.” Diversity in the enterprise context should be about creating an environment in which all people feel included, valued and free to achieve the best of which they are capable. A diverse IT audit team brings together different minds and perspectives to facilitate innovation, solve problems and advance learning—all of which, if harnessed properly, are likely to have a positive impact on audit quality and overall team performance.

**Endnotes**


2. Ibid.


**THE SUCCESS OR FAILURE OF A DIVERSITY AND INCLUSION PROGRAM CANNOT BE EFFECTIVELY QUANTIFIED WITHOUT METRICS IN PLACE.**


Earn Continuing Professional Education (CPE) credit hours online before the December deadline!

Learn more at: www.isaca.org/OnDemand-jv6
Those who have owned a house plant have probably noticed that no matter where the plant is placed, it grows toward the strongest source of light—a phenomenon called “phototropism.” Tropisms are defined as any growth in response to an environmental stimulus. They are found in nature in various forms, such as gravitropism (downward growth), hydrotropism (growth toward a water source) and aphototropism (growth away from a light source). Outside of the plant kingdom, the principles behind tropisms occur in places such as the economy, family life and the workplace.

Cybersecurity or IT professionals should seek out career opportunities that offer the right sorts of stimuli to enable their own growth. A positive corporate culture is one such stimulus. A well-rounded workforce development program is another. However, negative stimuli can be present as well trapping employees in situations that stifle growth, push coworkers away and drain the team of talent.

So, how do job candidates evaluate whether an organization has the right set of stimuli for their own development? There are a few critical questions to ask. How the employer answers should provide the insight needed to determine whether the job will support personal and professional goals or the organization has already put a ceiling on growth potential.

Those who lead a cybersecurity team may find these questions helpful in evaluating the opportunities their program provides their team members.

**Question 1: What Is the Multiyear Growth Plan for Someone in the Position?**

This is the answer candidates want to hear: Knowledge, skills and abilities (KSAs) are clearly defined for this role and there are expectations for growth. There is a clear plan for the professional development and career progression of someone in this position.

The term “KSAs” is most frequently used in the military, but the concept is universal. KSAs should serve as the baseline requirements for each position on the team. Organizations need defined KSAs to successfully map out how that role fits into the business and evolves over time.

Without KSAs, it is hard to set a structured plan for professional growth. KSAs can answer the questions, “What must candidates know and be able to do to be successful in this role?” and “What knowledge and skills must candidates learn to be...
ready for their next role?” Some see KSAs as restrictive or rigid, but they can be very empowering. Knowing exactly what must be delivered to move to the next level makes it much easier to seize the opportunity and move forward. In interviews, candidates should ask pointed questions about the specific skill sets and knowledge expected of the role and how they will evolve over time. If the interviewer can answer these questions, it shows that they have a plan for employees’ growth, goals to be achieved and opportunities for advancement.

To get started, the candidate should ask questions such as: What are the expectations for the growth of someone in this role? How will the skills of someone in this role evolve? How will career progression be measured? A careful examination of the job description may also be helpful. If only responsibilities or experience requirements are listed in the description, rather than the specific skills, it could be an indicator that KSAs are not in place for this position and the employee may be stuck carrying out the same tasks indefinitely, rather than advancing in his/her career.

Question 2: How Long Has the Interviewer Been With the Team? What Is Their Career Story?

This is the answer candidates want to hear: Team leadership is homegrown. Managers started their careers in the organization and worked their way up. Senior positions are rarely given to outside hires.

Panel interviews, in particular, provide a unique opportunity to quickly evaluate the amount of homegrown leadership on the team. A round-robin response from the interviewers can paint a picture of an organization that develops loyal, talented employees or it can describe a organization in which top talent flees at the first opportunity. Follow-up questions to learn more about the interviewers’ career journeys and experience at the organization can give additional insights into team structure and dynamics.

What is really important to uncover is if the team’s leaders and managers grew into their roles. If they have climbed a ladder into increasingly more skilled positions, that is a good indicator that there is a workforce development program in place. They are building a pipeline of skilled cybertalent, and new employees will be expected to develop new skills and advance within the enterprise. However, if it sounds like most of the team members are recent additions (especially those in leadership), the turnover rate for the team may be high, training may be limited and senior roles may be given to outside hires.

Listening to what the interviewers say about their experience at the organization can provide information that may not be available from their website, social media or Glassdoor. Questions that may help elicit this information focus on how long the interviewers have been with this organization, their background and how they got to their current position, and what made them decide to join the organization.

Question 3: What Approach Is Used to Build a Diverse, Well-Rounded Team?

This is the answer candidates want to hear: This enterprise is actively working to build a diverse team, looking for people with a variety of backgrounds, educations, skill sets and experiences. Diversity is important to this team and at this organization.

Enterprises that embrace diversity seek out a variety of backgrounds, skill sets, perspectives, experiences and ideas—all things cybersecurity needs. As an industry, and largely out of necessity, cybersecurity scores good marks for diversity of professional background: Many cybersecurity professionals come from backgrounds outside of the expected fields of information systems, computer science, etc. Today’s cyber leaders are just as likely to come from accounting, IT or the military. But, in other ways, diversity is severely lacking in cybersecurity. For instance, women make up only 11 percent of the global cyberworkforce.

Diversity is an interesting example of two types of tropisms. An organization that builds diverse teams is more likely to encourage the free collaboration
and sharing of ideas, which puts employees in an ideal position to learn new skills from their peer group and bring new ideas to the team (horizontal knowledge sharing, as opposed to vertical knowledge sharing). This results in upward growth as a professional. And when an organization embraces diversity, it also inspires employees to grow roots and build their career there.

Successful cybersecurity teams require unparalleled problem solving, lots of creativity and seamless teamwork. Diversity should be the engine that drives these outcomes. An organization that recognizes diversity as both the right thing to do and a way to improve security outcomes is also likely to be an organization with a robust program for developing diverse talent internally.

The global cybersecurity talent shortage has been well documented, and regulations, threats and technologies are constantly evolving. Most organizations have a few skills gaps on their cybersecurity team. How an organization handles this challenge can reveal a lot about its workforce development program.

Despite the shortage, some organizations still look for outside hires to fill gaps on their teams. Finding the right person can take months, if it happens at all, leaving the team with a significant gap in skills and the organization vulnerable. On the other hand, other organizations see a skills gap as a growth opportunity for an existing team member. These organizations have programs in place for ongoing and targeted skills development, constantly elevating employees to fill gaps and training up less experienced hires to fill open positions. This creates upward momentum for the whole team and a culture of shared goals, success and loyalty.

Finding out how the organization addresses these issues takes a little sleuthing. The job description for the open position should have some indicators of whether the organization is recruiting to fill a very specific gap. While the opportunity may be great now, it could mean the person hired will be stuck in that position for a while. During the interview, candidates should ask questions about how the organization tackles regulatory changes, new technologies, and new threats or risk. Does it rush to find someone new or will it start training team members on how to address these?

**Question 4: What Is the Strategy for Filling Openings on the Team? Is It to Train Up Existing Team Members or Look for an Outside Hire?**

This is the answer candidates want to hear: Existing team members are offered new opportunities first. The plan for filling skills gaps on the team is to train up existing team members to equip them with these skills.

Candidates should ask questions about the composition of the team, the team members’ backgrounds and what key team members bring to the table. Candidates should also ask pointed questions about the diversity programs at the organization. What initiatives does the organization have that encourage diverse hiring? Are there groups or programs that support diversity in the workplace? The types of programs the organization has in place are obvious indicators that it seeks out and supports diversity.

**THE TYPES OF PROGRAMS THE COMPANY HAS IN PLACE ARE OBVIOUS INDICATORS THAT IT SEEKS OUT AND SUPPORTS DIVERSITY.**

**Question 5: What Is the Training Program for the Team?**

This is the answer candidates want to hear: There is an established training program for team members at every level. Employees are given training opportunities, and there is an expectation that they will develop new skill sets.

This is a direct, obvious question, but it is one the candidate should save for last. The problem with a simple question about training is that every interviewer is ready for it. Interviewers know that training is important to most professionals, so they have a canned response ready—a response that may or may not be an accurate reflection of the training program in place.
So, candidates should ask questions that require specific answers. Ask the interviewers how the training is facilitated. Is it done in-house? Do employees attend external trainings? Is it online or in-person? How is training selected? Do employees have to find and choose the training they want? Are employees given a budget to self-select training or does the organization provide guidance? Is there a certain training provider the organization uses? Is training individual or team-based? Diving deep into how the organization's training program works will provide a more realistic picture of what it is actually doing when it comes to professional development. Candidates should want to see that the organization is making an investment in training and sees value in training the team as a whole. A budget is allotted to training and time is set aside for employees to develop new skills. The key is to go beyond the usual “Are there training opportunities?” questions and get into specifics.

**Taking the Next Step**

Many prepare for interviews by trying to anticipate the questions they might get asked. While this is important, preparing questions for the interviewer is equally important, especially regarding opportunities for professional development. The answers to these questions will help job seekers determine if a team is the right fit and potentially help them take a step forward in their career path. These questions will help job seekers find an organization that:

- **Welcomes diversity.** They are open to new ideas and different perspectives and realize that new and different solutions can be the answer to long-standing challenges.
- **Helps employees grow their skills.** Instead of looking to outside help for new challenges, opportunities are given to existing employees to learn by doing.
- **Guides employees in their career.** They see the importance of a good training program and help employees choose the courses they need to grow the career they want.

Look for an organization that provides the stimuli that helps employees grow, encourages them to put down roots, and expands their skill sets and knowledge. Then, new hires will experience what it is like to be a part of an organization and a team that wants to see team members succeed because they know that professional growth is critical to the success of the organization. Not only will employees find their work more fulfilling, but they will be excited about their future and the opportunities it holds.

**Endnotes**

Defining the Chief Digital Officer Using COBIT 5

The digital revolution’s pace is rapidly increasing, causing numerous disruptions and transformation in more and more industries. A key sign of its growing importance is the rise of a new kind of executive: the chief digital officer (CDO).¹

Discussions around C-level roles are not new. In fact, there is quite a contentious issue around the CDO and the chief information officer (CIO) and plenty of diverging references on both roles.² However, some contend that the CDO can be considered the ultimate realization of a type of CIO—more connected to business, more innovative and able to build relationships across all levels and functions of the organization.

It is still not clear what CDOs are expected to achieve, what their responsibilities are and how they can collaborate with their CIOs.³ The current lack of clear responsibilities of the CDO role and profile also creates some space for eventual conflicts with the CIO when they coexist. Clarifying the two is urgent and required to prevent future problems from occurring.

The responsibilities of the CDO role in the enterprise context can be identified and correlated with the CIO’s responsibilities using the Responsible, Accountable, Consulted and Informed (RACI) matrix from COBIT® 5. COBIT 5 provides benefit in this context because it is the only governance framework based in international governance standards (International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC] ISO/IEC 38500) and it draws a clear divide between governance and management.

Context

The digital world is changing rapidly and profoundly. Now more than ever, digital transformation (DT) plays a critical role in corporate strategy. DT encompasses a wide range of tasks and activities that are complex, cross-functional and interdependent, making it increasingly difficult for the CIO.⁴

João Catarino
Is finishing a master’s degree based on the topic of digital transformation. Catarino cowrote an article regarding research of governance frameworks for digital transformation in the public sector.

Isabel Rosa, Ph.D.
Is a national expert in the area of electronic public procurement in the European Commission and has 30 years of experience in information systems. She was the chief information officer of several public entities in Portugal and Macau (China). In Portugal, she was also the deputy secretary general and chairman of the ICT Committee of the Ministry of Public Works, Transports and Communications. She was a researcher of governance frameworks for digital transformation in the public sector in the field of a doctoral program of engineer and management.

Miguel Mira da Silva, Ph.D.
Is an associate professor of information systems at the Instituto Superior Técnico in the University of Lisbon (Portugal) and research group leader at INOV INESC Inovação.
Because organizations need to assign and spread managerial responsibilities adequately across top managers to ensure successful DT, a new generation of C-suite executives has emerged, including the CDO. Researchers suggest the CDO and the CIO not only collaborate closely, but also have a symbiotic and interdependent relationship.5

However, the ambiguity and contention that surrounds the definition of the CDO’s role persist. In particular, there is controversy between the CDO and CIO roles, which leads to internal difficulties in the organization, with an obvious impact on its ability to adapt to an increasingly unpredictable and demanding world.

Analyzing the differences between these two roles based on COBIT 5 draws a new vision of the responsibilities assigned to each role. The evaluation conducted through a user opinion study not only provided a positive evaluation of the proposal, but also resulted in valuable input for further work.

Research shows that the CDO’s primary responsibilities are those related to ensuring value optimization and stakeholder communication.

**CIO vs. CDO**

In the mid to late 1990s, the CIO was a senior executive who was able to understand new technologies and how to apply them to the business strategy. They were the link that intermediated the relationship between business leaders and the IT department.6

Meanwhile, a phenomenon was emerging: globalization. IT managers were faced with new challenges and, though IT had become better aligned with the business, IT executives needed to conduct rigorous analyses of return on investment (ROI) and make complex decisions. Moreover, significant technology expenditures needed to be justified. Naturally, not all CIOs were at ease with this challenge; the IT function demanded a leader who was able to understand the increased complexity of business and how to interact with the IT strategy, business strategy, risk management and finance.7

At this point, the future of CIOs began to be questioned. “CIOs who do great things in leading IT soon gain extra responsibilities. By helping business leaders to improve their businesses, the CIO becomes an obvious candidate to fill any open role that involves technology, process, or strong governance.”8 However, many new challenges, such as brand synergy, were new for the CIO.

Consequently, a growing number of organizations have introduced an additional position into their managerial grid—the CDO. An initial conceptualization of the CDO’s position suggests that its primary responsibilities are the strategic and communication aspects of DT, and, if the CDO and CIO positions coexist, the CDO should closely collaborate with the CIO. The CIO, in turn, deals with the technical aspects of DT. This means that, although the roles/responsibilities of the CDO and CIO are different, their relationship can be symbiotic and interdependent.9

Researchers identified four distinct CDO role types (digital innovator, advocate, evangelist and coordinator) and assessed the implications for the CIO role in the context of DT. In this research, the four distinct CDO role types are primarily determined by the CIO’s role orientation and the perceived implications of digitalization.10

**Proposal**

Now that DT is sure to reach every organization, it is important to note that governance is essential for successful DT.11 To differentiate between management and governance, one researcher associates governance to the context of change or transformation. Thus, governance guides developments that lead to a new (or partly new) organization that needs to be managed.12

A set of responsibilities is proposed for the emerging CDO role for the governance of DT and an adjustment of the CIO’s responsibilities in the new context. This proposal is based on two fundamental principles: simplicity and ease of use. Hence, it is relevant to use well-known and extensively accepted frameworks. This is made possible by using the RACI matrix from COBIT 5.
To identify the responsibilities of the CDO and CIO within the enterprise context, the RACI matrix is used. COBIT 5 already identifies responsibilities for the CIO in its 37 processes. COBIT 5 describes the responsibilities associated to the key practices that make up each process as a RACI matrix.

The COBIT 5 framework can be considered to be in line with the governance of DT since COBIT 5 was designed for IT governance with a specific goal of aligning IT with the business and, subsequently, to generate value to the organization. Moreover, COBIT 5 makes a very pragmatic distinction between governance processes and management processes—a positive aspect in change/transformation and, more specifically, in DT.

Considering the concept of the CDO as the manager of digital transformation enables a conclusion that this role should be grounded in governance principles. Governance provides direction. Management provides operations. This leads to a vision of the role of CDO as a bridge between IT and the business (figure 1).

As explained, the CIO’s responsibilities are reassessed should the role of the CDO be introduced in the organizational context.

Given the premise that derives from the concept of governance as the functional area that manages change and transformation, and considering that the CDO’s role is, by definition, DT management, only the governance processes under the COBIT 5 framework have been studied: EDM01 Ensure Governance Framework Setting and Maintenance, EDM02 Ensure Benefits Delivery, EDM03 Ensure Risk Optimization, EDM04 Ensure Resource Optimization, and EDM05 Ensure Stakeholder Transparency.

With the introduction of the new CDO role, the new proposed distribution is shown in figure 2.

This proposal is based on the following basic vectors:

- The CDO is responsible for the governance processes.
- The responsibilities of EDM04 are shared by the CDO and the CIO due to the direct link with the infrastructure management responsibilities of the CIO.
- Both roles are responsible for evaluating the benefits since this activity requires both perspectives, from the business and deep IT knowledge.
- Both roles share the responsibility of evaluating and monitoring risk management, owing to the wide scope of the source of risk.
- Although the CIO is no longer responsible in all remaining activities, the CIO should be consulted except for directing and monitoring the stakeholders’ communication. This is for two reasons: This is a CDO core activity, and the CIO should not duplicate efforts, instead concentrating on his or her core activities.

This proposal gives the CDO stronger responsibility on the three processes EDM01, EDM02 and EDM05. It further grants shared responsibility with the CIO on the remaining two processes: EDM03 and EDM04.
Evaluation

Given the controversy of this topic, the assessment of the proposal was gathered via a user opinion study. Not only was it important to obtain a proposal assessment, it was also critical to understand how the community closest to the topic sees the CDO and the CIO roles.

Fifteen people replied to the questionnaire, all senior professionals in their line of work, with an average career span of approximately 22 years. As for geographic diversity, 13 of the respondents are Portuguese, one is Brazilian and one is Dutch. It should be added that in the Portuguese group, three respondents work abroad in several countries at the same time. The organization types of the respondent group are also mixed: Five are in public service and 10 are in private institutions. In terms of area of job functions, the respondents include four chief executive officers (CEOs), three digital professionals, three academicians and five working in information and communication technology (ICT).
The questionnaire was designed to be self-explanatory and contained five sections: the respondent's characteristics, views on the topic, general proposal assessment, detailed proposal assessment, and identification of three functions and three characteristics associated with the CDO and CIO.

The questionnaire had three types of questions: multiple choice, open ended and scaled (graded on a scale from 1 to 10, in which 1 = Completely disagree and 10 = Completely agree). This last group contains the most relevant component of the proposal assessment: the responsibilities assigned to each role (figure 3).

The analysis of the results shows some interesting conclusions.

Digital professionals are, in general, more supportive of the proposal, while those more connected to ICT are, in general, less supportive. The reason for this is the growing controversy that the role of the CDO is a threat to that of the CIO and the sense of rivalry between these two roles that transpires from the media.

In one of the questions, respondents were asked to list three characteristics for each profile. Although they are described differently, there is a convergence of opinions from which the following stand out:

- **CDO profile**—Business-oriented, leadership skills, visionary, higher risk profile, strategic thinking, strong relationship builder, problem-solving

<table>
<thead>
<tr>
<th>Governance Processes</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EDM01: Ensure Governance Framework Setting and Maintenance</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate the governance system</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Direct the governance system</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Monitor the governance system</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td><strong>EDM02: Ensure Benefits Delivery</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate value optimization</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Direct value optimization</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Monitor value optimization</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td><strong>EDM03: Ensure Risk Optimization</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate risk management</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Direct risk management</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Monitor risk management</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td><strong>EDM04: Ensure Resource Optimization</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate resource management</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Direct resource management</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Monitor resource management</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td><strong>EDM05: Ensure Stakeholder Transparency</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate stakeholder reporting requirements</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Direct stakeholder communication and reporting</td>
<td>R</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Monitor stakeholder communication</td>
<td>R</td>
<td>I</td>
<td></td>
</tr>
</tbody>
</table>
attitude, reward assessment capabilities, innate design/lean thinking

- **CIO profile**—IT-oriented, focused, detail-oriented, results-oriented, collaborative, tech savvy, business supporter, ability to execute on change, ability to translate strategy into execution, technical leadership

This shows how these two roles require substantially different characteristics.

Regarding the functions exercised by the CDO and the CIO, one of the questions was to list the main three functions. The following are worth noting:

- **CDO functions**—Define the digital strategy/vision, align/converge the digital strategy with the corporate strategy, create a digital culture in the enterprise, disrupt, transform to digital, change management

- **CIO functions**—Implement IT projects, build IT strategy, change management, establish a technologic landscape that incorporates future business needs with less impact, ensure time to market, ensure an adequate IT governance framework

Despite all the controversy that the proposal assessment raises, it is rather positive overall.

**Figures 4 and 5** show the assessment average scores obtained for the CDO and the CIO, respectively.

The results in **figure 6** show a higher agreement on the responsibilities of the CDO in the processes regarding value optimization, stakeholders’ communication and the governance system, in line with the previously stated conclusions about the CDO’s primary focus on strategic and communication aspects.14

In short, the results of the questionnaire show that the COBIT 5 RACI matrix can be a very important tool in defining/redefining both roles in the organizational context of DT. Indeed, its formulation can lead to a rethinking of the current situation. What is clear from **figures 4 and 5** is that the agreement on the CIO’s responsibilities is lower when the responsibility shifts from R (responsible) to C (consulted) or I (informed). In the case of the CDO, which is responsible (R) for all processes, the clear disagreement falls on the EDM04 process. Interestingly, though, this process was proposed with shared responsibility by the CIO, and it was precisely in this process that the CIO achieved the most in-sync answers.

**Conclusion**

Clear roles at the C-level are essential to boost the enterprise’s capabilities in times of disruption.

**Figure 4—Average Evaluation of CDO Responsibilities**

<table>
<thead>
<tr>
<th>CDO Average Score</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor value optimization – R</td>
<td>9.54</td>
</tr>
<tr>
<td>Evaluate value optimization – R</td>
<td>9.35</td>
</tr>
<tr>
<td>Direct value optimization – R</td>
<td>9.26</td>
</tr>
<tr>
<td>Direct stakeholder communication and reporting – R</td>
<td>9.00</td>
</tr>
<tr>
<td>Monitor stakeholder communication – R</td>
<td>8.82</td>
</tr>
<tr>
<td>Evaluate stakeholder reporting requirements – R</td>
<td>8.27</td>
</tr>
<tr>
<td>Evaluate the governance system – R</td>
<td>8.10</td>
</tr>
<tr>
<td>Monitor the governance system – R</td>
<td>8.09</td>
</tr>
<tr>
<td>Direct the governance system – R</td>
<td>7.91</td>
</tr>
<tr>
<td>Evaluate risk management – R</td>
<td>7.93</td>
</tr>
<tr>
<td>Monitor risk management – R</td>
<td>7.33</td>
</tr>
<tr>
<td>Direct risk management – R</td>
<td>6.97</td>
</tr>
<tr>
<td>Monitor resource management – R</td>
<td>5.90</td>
</tr>
<tr>
<td>Evaluate resource management – R</td>
<td>5.63</td>
</tr>
<tr>
<td>Direct resource management – R</td>
<td>5.55</td>
</tr>
</tbody>
</table>

0,00 2,00 4,00 6,00 8,00 10,00
The research described here, particularly the responses of practitioners who participated in the proposal assessment, shows that using the RACI matrix to define the CDO’s and the CIO’s responsibilities is quite feasible and, above all, very useful to clarify the boundaries between the two roles. The overall scores for both proposals were very positive: 7.62 for the CIO and 7.96 for the CDO, on a scale of 1-10 points.

This study focused solely on the CDO and CIO responsibilities in the context of the COBIT 5 governance processes. The first major proposal evaluation findings were that most people find it difficult to clearly distinguish between governance and management.

This difficulty implies that their functions/activities, objectives and required skills are not evident. It is,
therefore, more difficult to understand the reason for the predominant connection between the CDO and the governance processes and the CIO and the management processes.

On the other hand, the responses to the study showed that it was easier to understand the connection between governance and transformation.

It was also clear that although the management processes were not the subject of this study, they should also be reviewed. Though the predominance of responsibilities of the CIO role at this level is more predictable, this is not to say that in some processes responsibilities could not be shared, in particular: APO02 Manage Strategy, APO04 Manage Innovation and APO08 Manage Relationships.

It is important to stress that this study is still taking its very first steps, and it takes more than qualitative studies to consolidate the findings on this topic. It will be useful to understand these findings if frameworks of digital enterprise governance emerge and determine how both roles will be addressed by the community of practitioners.

Authors’ Note

Opinions expressed in this article are the authors’ own and do not necessarily represent the views of any entity.

Endnotes


4 Ibid.

5 Ibid.


7 Ibid.


9 Op cit Horlacher and Hess


14 Op cit Horlacher and Hess
A Heightened Sense of Awareness
What the Internal Auditor Should Know About Information Security Awareness Training

According to the US National Institute of Standards and Technology (NIST), each individual in an organization who owns, uses, relies on, or manages information and information systems must fully understand his or her specific security responsibilities.¹

One of the most important tools an organization has (or should have) to reach that state of readiness is an information security awareness training program.

Even though internal auditors may not be performing an audit of the security awareness training program specifically, they should be familiar with the elements of a good awareness program regardless of the business area at which they are looking. If there are issues in a security-related area, awareness training may be one place they can look to provide recommendations.

The key characteristics of an information security awareness training program that an internal auditor should be aware of include the extent to which the program is supported by management, the content of the training itself, how that training is delivered and how the organization measures success for the program.

Management Support

A successful information security awareness training program must have the support of senior management for the obvious reason that it requires the commitment of resources (money and employee hours). Beyond that, senior management must see to it that:

- The program content and delivery are well suited to the needs of the organization.
- The training is understood and retained well enough to influence employee behavior.
- The organization receives value from the program in terms of mitigating security risk.

Finally, and perhaps most important, senior management should reinforce the awareness training by setting a good top-down example in their behaviors and attitudes. “The critical success factor [for an information security awareness program] is...”

Wade Cassels, CISA, CFE, CIA, CRMA
Is a senior IT auditor at Nielsen. He supports Nielsen’s IT general controls external audit engagement and the audit reporting and communications functions for Nielsen Internal Audit.

Kevin Alvero, CFE
Is senior vice president of internal audit at Nielsen. He leads Nielsen’s global internal quality audit program and its industry standards compliance initiatives, spanning the company’s television, digital, and consumer products and services.

Randy Pierson, CISA
Is a senior IT auditor at Nielsen and has worked in the media and entertainment industry since 2011. Before joining Nielsen, he worked as an auditor with Ernst & Young, where he served organizations across the media industry, including television, Internet and mobile audience research. Pierson also served as compliance officer for the digital media company Pixalate.
how well top management acts as role models for its employees,” writes V. J. Srinivas in a recent ISACA Now blog post. “Their actions will influence and enhance policy compliance and awareness levels among employees.”

Content
The most important aspect of good security awareness training content is making sure it is customized to the audience based on their job area, role and user level. It would not be productive, in fact, it would be counterproductive, to teach general staff about security threats and policies/processes that are specific to technical users, such as programmers or personnel who maintain system architecture. In addition to the obvious benefit of aiding retention, keeping training at an appropriate technical level also helps to ensure that knowledge of more complex and technical security processes is limited in its exposure to those who need to know. However, it is important to provide all trainees enough visibility to understand how their everyday roles fit into the big picture of the organization’s overall security risk management. All users should understand, for example, not just that they are required to update their password(s) regularly, but they should also be able to articulate how password protocols help protect them and the organization.

Even though security awareness training is often provided by a third-party vendor, it is important that multiple areas of the organization contribute to the development of the training content to ensure that the content is well suited to the organization’s needs and the risk environment in which it operates. Input related to content should not only come from places such as security, IT, information security and legal, but also from operational leaders who can provide insight into how general users interact with security risk/threats in the course of their day-to-day duties so that the training provider (whether internal or third party) can cater to that risk. The internal auditor should also be aware if his or her organization is practicing sound vendor risk management practices. As one author noted, “Companies must perform [due diligence] on any organization they consider to provide outsourced online training to employees.”

From a content perspective, good training should consist of real-world examples that are relatable to the trainees’ everyday work. It should also include real-world case studies that help to reinforce the reality that security breaches do happen and demonstrate how the organization can be impacted.

Finally, awareness training must be compliant with any relevant standards or regulations (such as the US Federal Information Security Management Act [FISMA]), based on the organization’s geography, industry type, etc.

Format/Delivery
In the cat-and-mouse game of protecting organizational assets, security threats are constantly evolving, so security awareness training is never done. It should be performed on a routine basis and updated regularly. Generally, trainees are better able to understand and retain smaller amounts of information presented in regular increments.

The training should also come from a variety of different delivery methods. An article published by the SANS Institute says,

“One of the best ways to make sure company employees will not make costly errors in regard to information security is to institute company-wide security-awareness training initiatives that include, but are not limited to classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of company security policy, procedure and best practices.”

In-person classroom training, which may be the most resource intensive and, therefore, the least frequent, can be complemented by more frequent online training (modules or live virtual sessions) and by even more frequent email or newsletter.
communications. Using these different types of delivery methods in concert allows organizations to control costs, disseminate information with agility and achieve understanding by different types of learners. Incorporating user communities also gives employees access to support for questions or issues as they arise.

Regardless of the delivery type, there should be some interactive element to the training. Interactivity helps to ensure participation and promote retention. Online modules may have pop-up quizzes or other checks for understanding, for example. In live classroom or live virtual training, attendees should have the opportunity to ask questions.

Measurement

A good security awareness program must have metrics that help management make informed judgments about its effectiveness. Generally, these metrics fall into three main categories:

- **Participation**—Are the right people receiving the training when needed? This is the easiest part of the program to measure and, although participation alone is not sufficient to judge success, it is, nevertheless, important to track.

- **Retention**—Are trainees understanding the material that is being taught? Not only is this important to capture on a session-by-session basis, but tracking this information over time will help management and vendors make incremental improvements to the content and structure of the awareness training program.

- **Compliance**—Are employees carrying the knowledge forward into their roles? There are a number of ways organizations can measure if awareness training is affecting employee behavior, including incident tracking and review, penetration testing (i.e., hacking, phishing, social engineering), and internal audits of adherence to policies such as data retention, password and off-boarding protocols.

However, using these measurements to make an assessment about the value of the training program to the organization—its return on investment (ROI)—can be one of the more challenging aspects of managing the program. For the internal auditor, who is conditioned to think of risk in terms of likelihood and impact, it is helpful to consider whether the training program is mitigating either, or both.

For example, if having an awareness program is a matter of compliance, then avoiding the costs of noncompliance (i.e., fines, reputational damage) obviously contributes to ROI. Meanwhile, if the estimated financial impact of an event (e.g., a particular information security breach) is known based on the organization’s risk assessment process, then a change in the organization’s level of susceptibility (i.e., likelihood), which can be measured, can provide management with an idea of the return they are getting from awareness training.

The key is having the measurements in place on which to base ROI calculations prior to implementing the training. As one expert notes, “If you have a concrete (or at least evidence-based) way to track susceptibility, measuring ROI is simple.”

Maturity

In 2016, SANS introduced the Security Awareness Maturity Model (figure 1). The internal auditor should understand where on the spectrum his or her organization falls, but, perhaps more important, the internal auditor should determine whether or not a maturity model is being utilized by management to guide the content, frequency, delivery and measurement of the security awareness training program over time. Per the SANS website, the spectrum of maturity levels are defined as follows:

- **Nonexistent**—Program does not exist. Employees have no idea that they are a target, that their actions have a direct impact on the security of the organization, do not know or understand organization policies, and easily fall victim to attacks.
• **Compliance focused**—Program is designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad hoc basis. Employees are unsure of organizational policies and/or their role in protecting their organization’s information assets.

• **Promoting awareness and behavior change**—Program identifies the training topics that have the greatest impact in supporting the organization’s mission and focuses on those key topics. Program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home and while traveling. As a result, people understand and follow organization policies and actively recognize, prevent and report incidents. Behavior can begin to be changed in as early as several weeks, depending on the behavior being targeted.

• **Long-term sustainment and culture change**—Program has the processes, resources and leadership support in place for a long-term life cycle, including, at a minimum, an annual review and update of the program. As a result, the program is an established part of the organization’s culture and is current and engaging. It takes a minimum of 3-5 years to effectively change culture.

• **Metrics framework**—Program has a robust metrics framework to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. This stage does not imply metrics are not part of every stage (they are). This stage reinforces that to truly have a mature program, it must have metrics to demonstrate success.

**Conclusion**

For an organization’s employees to react appropriately to the security threats they encounter and to avoid unknowingly becoming a security threat themselves, they must receive regular, relevant and engaging information security awareness training. That is why the internal auditor should be able to recognize and articulate the elements (or missing elements, as the case may be) of an effective security awareness training program that delivers value to the organization.

---

**Figure 1—Security Awareness Maturity Model**

Endnotes


Skill Acquisition in a Rapidly Evolving Workplace

The cybersecurity skills gap has been on the surface of employers’ awareness for several years. The ability to meet security objectives given the skills gap is compounded by the moving target created by evolution in the workplace. While factors such as age or gender definitely contribute to the changing workplace, it is the rapid pace of evolution related to new technology that captures the attention of technologists looking to future proof their careers. As organizations adopt new technologies, a gap is created between the new skills required of security personnel and IT audit staff and the skills these practitioners hold.

In ISACA’s State of Cybersecurity 2018: Workforce Development survey, respondents indicated that the greatest hiring demand is expected at the technical security level for individual contributors, not the management or executive level (figure 1). Of those responding, 77 percent indicated increased staffing needed at this level compared to 76 percent reporting no additional staffing required at the executive or C-suite level.

One of the key enterprise takeaways cited by the report is that “the increasing need for skilled security personnel validates investment in existing staff, including education, training, skill development and certification, particularly in technically relevant areas.” In looking to the future, a potential bottleneck in upward mobility may exist for those entering the field now. This could be attributable to increased competition for those higher-level positions as a larger group of practitioners seeks that next career progression. Also, trends toward automation may play a role in that potential bottleneck. So, those practitioners looking to future proof their careers may explore the following options.

Balance Interpersonal Skills With Technical Skills

If technologists include acquisition or enhancement of interpersonal skills as part of their career planning, inclusion is more likely to be incidental rather than a skill set that is intentionally developed. After all, people tend to believe that they work collaboratively with others. Given workforce diversity in age, gender, national origin, technical background and other factors, collaboration is indeed a critical interpersonal skill; however, it is not the only interpersonal skill required to future proof a career in technology. Balancing interpersonal skills with their technical skills will serve technologists in their current roles and continue to serve them as their careers progress.

Figure 1—Hiring Demand Organizational Level

<table>
<thead>
<tr>
<th>Level</th>
<th>Increased staff needed</th>
<th>No change in staff needed</th>
<th>Decreased staff needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual contributor, technical security</td>
<td>77%</td>
<td>21%</td>
<td>2%</td>
</tr>
<tr>
<td>Individual contributor, nontechnical security</td>
<td>58%</td>
<td>39%</td>
<td>4%</td>
</tr>
<tr>
<td>Security manager</td>
<td>70%</td>
<td>26%</td>
<td>3%</td>
</tr>
<tr>
<td>Senior manager or director of security</td>
<td>76%</td>
<td>21%</td>
<td>3%</td>
</tr>
<tr>
<td>Executive or C-suite security (e.g., CISCO)</td>
<td>80%</td>
<td>20%</td>
<td>0%</td>
</tr>
</tbody>
</table>

In 2018, for which of these levels do you see the hiring demand increasing, decreasing or remaining the same?
Key Skill Acquisition
Although the greatest hiring demands are at the executive or C-suite level now, practitioners who aspire to positions at those levels should develop public speaking skills. At the executive level and beyond, speaking at board meetings and to internal and external audiences is expected. Public speaking skills can be learned through any number of groups dedicated to that skill and honed by volunteering to speak at meetings of professional associations such as ISACA®.

Strategically Develop Skills That Can Be Objectively Demonstrated
Given the rapid pace at which new technologies are adopted, it is impractical to be an expert in all things IT. As a result, the technologist benefits from taking a tactical approach to skill development. In their current positions, technologists should ensure alignment of technical skills with their organizations’ strategic objectives. For example, if an organization has adopted a hybrid cloud strategy, a technologist should have a solid understanding of capabilities and challenges of public cloud vs. on-premise cloud solutions. Enhancing knowledge through selected readings or online tutorials may be ways to develop skills for these scenarios. Depending on the technologist’s role, that may be sufficient.

Should the technologist want to be viewed as a subject matter expert by the organization, however, objective demonstration of skills may be a better path to take. Objectively demonstrating a skill can be achieved through practical work experience in the subject area. Alternatively, objective demonstration of skills can be shown through certifications; a certification demonstrates a skill set whereas a one-off course demonstrates proficiency. Practitioners should ensure that the certifications pursued are recognized and appreciated in their industries as well as by their organizations.

Having identified ways to develop skills in an evolving workplace, practitioners should leverage their organizations’ existing platforms to document their skills. It is not uncommon for organizations’ human resources departments to maintain profiles of their employees. The purpose of these platforms is to be informed as employees develop educationally by attaining degrees or expand their skills through new certifications. The idea is that as new internal opportunities requiring these degrees or skills arise, employees will be considered for those new opportunities.

Key Skill Acquisition
Ensure that skills can be objectively demonstrated.

Build and Maintain Partnerships Around Emerging Technologies
Leveraging participation in professional organizations and e-publications from groups that report on emerging technologies are ways for practitioners to learn about new technologies. Awareness of new technologies is critical as it allows practitioners to consider if there is a suitable fit for the technology in their organizations. If so, the practitioner has lead time to consider any challenges should the technology be considered and develop possible solutions to those challenges. Similar to monitoring emerging technologies, practitioners should develop a way to monitor pending compliance requirements. Developing an understanding of those requirements enables the technologist to analyze how existing technology and new technology can support new compliance requirements.

Key Skill Acquisition
Have a plan to ensure awareness of new technologies as they emerge.

Conclusion
The rapid pace of change in the workplace makes this an exciting time to be an IT practitioner. The need to acquire new skills at a fast pace adds an element of challenge to the excitement. Armed with a tactical plan to align skill development with their organization’s strategic objectives, to remain cognizant of the importance of interpersonal skills, and to leverage internal and external professional relationships to monitor emerging technologies, practitioners can meet the challenge of developing skills that keep pace in rapidly changing environments.

Endnotes
2 Ibid., p. 10
3 Ibid., p. 11
4 Ibid., p. 10
Crossword Puzzle
by Myles Mellor
www.themecrosswords.com

Across
1. Model that replaced the centralized (mainframe) model
6. Customer care system, abbr.
8. Institute that monitors standards and technology, abbr.
9. The N in NGFW
10. ______ware, unnecessarily added software
12. Meeting lists
13. Jotted down
16. German software company
18. Oversimplifies, 2 words
20. Tech experts
21. Back when
22. Sectioned
24. Tear into pieces (2 words)
25. Historical period
27. ______ source
28. Formal and explicit approval
33. Video device, for short
34. Credit card company
35. Security model in which all resources of a network are accessed securely. 2 words
38. Core belief
39. Unit of force
40. Outlook recommended by futurist Mark Stevenson

Down
1. The D in DoS attacks
2. Organized sets of principles
3. Complaints
4. Magnate
5. Forum activities
6. The Internet of remote servers used for storage, 2 words
7. School near Harvard, abbr.
11. Changed to survive in different conditions
14. One who plots bad stuff
15. Extremely popular
17. Goal
18. Statistic
19. Presides over a debate
22. Sleeps at the switch, perhaps
23. One thousand dollars, in slang
24. Computer memory
26. What Blackberry started as
29. IBM products
30. States
31. Do not waste
32. Numerical piece of data, abbr.
36. Brazilian city
37. Einstein’s birthplace
38. Moral strength in Confucianism

Answers on page 58
TRUE/FALSE

PEARCE ARTICLE
1. ISACA’s IT portfolio management paradigm focuses on return on investment, but does not consider the mix of types of technology in which investment may be made.
2. One method users may find helpful to visualize IT investment variability and the risk of failure is the Monte Carlo simulation.
3. The IT investments known as “cash cows” are those that provide higher returns than they should for the risk they bear.

TAMMINEE DI ARTICLE
4. According to COBIT® 5 for Risk, key performance indicators (KPIs) are metrics capable of showing that the enterprise is, or has a high probability of being, subject to a risk that exceeds the defined risk appetite.
5. In the three-lines-of-defense model, the second line of defense is an independent corporate risk function.
6. In developing a risk register, many inputs need to be considered, including corporate objectives and policies defined by senior management and authoritative sources and standards.

BRUNSWICK ARTICLE
7. A robust and well-designed managed file transfer (MFT) program and integrated platform can be useful to any organization involved in data movement, which makes it especially helpful for enterprises that must comply with the EU’s General Data Protection Regulation (GDPR).
8. Organizations may not have to exert quite as much effort as expected to remain compliant with GDPR because only a few selected actions taken on data are technically considered “processing” and, therefore, subject to its regulations.
9. GDPR’s Article 30 specifies that records of processing activities must be maintained, noting specifically the type of data processed, but not the purpose for which the data are used.

ZONGO ARTICLE
10. Blockchains are distributed across many participants in the network, but this decentralized approach is backed up by use of a centralized repository.
11. Regulators are beginning to address the lack of global laws to govern digital currencies and initial coin offerings (ICOs). This is a difficult task because ICOs can attract participants from around the world, raising the possibility of possible conflicts of laws across jurisdictions.
12. Because ICOs lack historical performance data or credible cash-flow predictions, investors will find it difficult to benchmark ICO valuations.
13. Blockchain is just one of many recent examples of an emerging technology. While many organizations feel pressured to stay ahead of technological advances, they need not feel quite so driven because research reported in the Harvard Business Review indicates that organizations that neglect digital innovation show no effects on their revenues and earnings.

HO ARTICLE
14. Placing cybersecurity within information security, organizationally speaking, can help eliminate duplication of activities, whereas structuring them as equal counterparts may result in overlap of responsibilities.
15. The key to making the lines-of-defense model effective is to ensure that the lines remain truly separate, not sharing reports or results between or among them.

SERRES ARTICLE
16. The knowledge, skill and experience of the information security staff are the primary factors on which organizations base their security technology acquisitions.
17. Risk management must be embedded in cybersecurity decisions to ensure that risk, rather than solely technological criteria, guides those decisions.

ONAL ARTICLE
18. The use of the word “holistic” in the article’s definition of the term “data governance” makes it clear that data governance applies to all data within the organization, including data originating from outside sources.
19. Solvency II and International Financial Reporting Standards (IFRS) are data-focused regulations that apply only to the insurance industry.
### TRUE OR FALSE

<table>
<thead>
<tr>
<th>PEARCE ARTICLE</th>
<th>TAMMINEEDI ARTICLE</th>
<th>HO ARTICLE</th>
<th>SERRES ARTICLE</th>
<th>BURNSWICK ARTICLE</th>
<th>ONAL ARTICLE</th>
<th>ZONGO ARTICLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>4.</td>
<td>12.</td>
<td>13.</td>
<td>7.</td>
<td>18.</td>
<td>10.</td>
</tr>
<tr>
<td>2.</td>
<td>5.</td>
<td>14.</td>
<td>15.</td>
<td>8.</td>
<td>19.</td>
<td>11.</td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td>16.</td>
<td>17.</td>
<td>9.</td>
<td>20.</td>
<td></td>
</tr>
</tbody>
</table>

**Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current Journal subscribers. An electronic version of the quiz is available at www.isaca.org/cpequiz; it is graded online and is available to all interested parties. If choosing to submit using this print copy, please email, fax or mail your answers for grading. Return your answers and contact information to ISACA Support or by fax to +1.847.253.1755. Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address. You will be responsible for submitting your credit hours at year-end for CPE credits. A passing score of 75 percent will earn one hour of CISA, CRISC, CISM or CGEIT CPE credit.**

---

**THE ANSWER FORM**  
Based on Volume 4, 2018

**Name**  
PLEASE PRINT OR TYPE

**Address**

**CISA, CRISC, CISM or CGEIT #**

**Answers:** Crossword by Myles Mellor  
See page 56 for the puzzle.
ISACA Member and Certification Holder Compliance

The specialized nature of information systems (IS) audit and assurance and the skills necessary to perform such engagements require standards that apply specifically to IS audit and assurance. The development and dissemination of the IS audit and assurance standards are a cornerstone of the ISACA® professional contribution to the audit community.

IS audit and assurance standards define mandatory requirements for IS auditing. They report and inform:

- IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession’s expectations concerning the work of practitioners
- Holders of the Certified Information Systems Auditor® (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder’s conduct by the ISACA Board of Directors or appropriate committee and, ultimately, in disciplinary action.

ITAF™, 3rd Edition (www.isaca.org/itaf) provides a framework for multiple levels of guidance:

IS Audit and Assurance Standards

The standards are divided into three categories:

- General standards (1000 series)—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments and deal with the IS audit and assurance professional’s ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- Performance standards (1200 series)—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- Reporting standards (1400 series)—Address the types of reports, means of communication and the information communicated.

Please note that the guidelines are effective 1 September 2014.

General
1001 Audit Charter
1002 Organizational Independence
1003 Professional Independence
1004 Reasonable Expectation
1005 Due Professional Care
1006 Proficiency
1007 Assertions
1008 Criteria

Performance
1201 Engagement Planning
1202 Risk Assessment in Planning
1203 Performance and Supervision
1204 Materiality
1205 Evidence
1206 Using the Work of Other Experts
1207 Irregularity and Illegal Acts

Reporting
1401 Reporting
1402 Follow-Up Activities

IS Audit and Assurance Guidelines

The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorization as the standards (also divided into three categories):

- General guidelines (2000 series)
- Performance guidelines (2200 series)
- Reporting guidelines (2400 series)

General
2001 Audit Charter
2002 Organizational Independence
2003 Professional Independence
2004 Reasonable Expectation
2005 Due Professional Care
2006 Proficiency
2007 Assertions
2008 Criteria

Performance
2201 Engagement Planning
2202 Risk Assessment in Planning
2203 Performance and Supervision
2204 Materiality
2205 Evidence
2206 Using the Work of Other Experts
2207 Irregularity and Illegal Acts
2208 Sampling

Reporting
2401 Reporting
2402 Follow-Up Activities

IS Audit and Assurance Tools and Techniques

These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programs, reference books and the COBIT® 5 family of products. Tools and techniques are listed under www.isaca.org/itaf.

An online glossary of terms used in ITAF is provided at www.isaca.org/glossary.

Prior to issuing any new standard or guideline, an exposure draft is issued internationally for general public comment.

Comments may also be submitted to the attention of the Director, Content Strategy, via email (standards@isaca.org); fax (+1.847.253.1755) or postal mail (ISACA International Headquarters, 1700 E. Golf Road, Suite 400, Schaumburg, IL 60173, USA).

Links to current and exposed ISACA Standards, Guidelines, and Tools and Techniques are posted at www.isaca.org/standards.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of these products will assure a successful outcome. The guidance should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the control professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or IS environment.
CISA, CRISC, CISM and CGEIT Review Manuals Are Available as eBooks!

Get the training you need. Prepare to obtain your CISA, CRISC, CISM or CGEIT certification and be recognized among the world’s most-qualified information systems professionals. ISACA’s Online Review Courses provide internet accessible, on-demand instruction and are ideal for preparing you and fellow audit, assurance, control, security and cybersecurity professionals for ISACA’s certification exams.

VISIT ISACA.ORG/EXAMONLINEREVIEW TO LEARN MORE.
FEATURED PUBLICATIONS

CISA® Review Manual, 26th Edition

The CISA Review Manual 26th Edition is a comprehensive reference guide designed to help individuals prepare for the CISA exam and understand the roles and responsibilities of an information systems (IS) auditor. The manual has been revised according to the 2016 CISA Job Practice and represents the most current, comprehensive, peer-reviewed IS audit, assurance, security and control resource available worldwide.

The 26th edition is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

- The Process of Auditing Information Systems
- Governance and Management of IT
- Information Systems Acquisition, Development and Implementation
- Information Systems Operations, Maintenance and Service Management
- Protection of Information Assets

The CISA Review Manual 26th Edition features an easy-to-navigate format. Each of the five chapters has been divided into two sections for focused study. Section one of each chapter contains the definitions and objectives for the five areas, as well as the corresponding tasks performed by IS auditors and knowledge statements (required to plan, manage and perform IS audits) that are tested on the exam. It also includes:

- A map of the relationship of each task to the knowledge statements
- A reference guide for the knowledge statements, including the relevant concepts and explanations
- References to specific content in section two for each knowledge statement
- Self-assessment questions and explanations of the answers
- Suggested resources for further study

Print Product Code: CRM26ED
Ebook Product Code: EPUB_CRM26ED
Member Price: $105.00
Non-member Price: $135.00
Print book available in Chinese, French, Italian, Japanese and Spanish.


Many questions have been revised or completely rewritten to be more representative of the CISA exam question format and/or to provide further clarity or explanation of the correct answer. These questions are not actual exam items but are intended to provide CISA candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam.

To assist candidates in maximizing study efforts, questions are presented in the following two ways:

- Sorted by job practice area—Questions, answers and explanations are sorted by the CISA job practice areas. This allows the CISA candidate to refer to questions that focus on a particular area as well as to evaluate comprehension of the topics covered within each practice area.
- Scrambled as a sample 150-question exam—150 of the 1,000 questions included in the manual are selected to represent a full-length CISA exam, with questions chosen in the same percentages as the current CISA job practice areas. Candidates are urged to use this sample test to simulate an actual exam and to determine their strengths and weaknesses in order to identify areas that require further study. Answer sheets and an answer/reference key for the sample exam are also included. All sample test questions have been cross-referenced to the questions sorted by practice area, making it convenient for the user to refer back to the explanations of the correct answers.

Print Product Code: QAE11ED
Member Price: $120.00
Non-member Price: $156.00
Print book available in Chinese, Italian, Japanese, Spanish and Turkish.
CISA® Review Questions, Answers & Explanations Database—12 Month Subscription

The CISA Review Questions, Answers & Explanations Database is a comprehensive 1,000-question pool of items that contains the questions from the CISA Review Questions, Answers & Explanations Manual 11th Edition. Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. The database is available via the web, allowing CISA Candidates to log in at home, at work or anywhere they have Internet connectivity.

Database Product Code: XMXCA15-12M
Member Price: $185.00
Non-member Price: $225.00
MAC and Windows compatible.


The CRISC Review Questions, Answers & Explanations Manual, 5th Edition has been expanded and updated to include even more practice questions. This study aid is designed to familiarize candidates with the question types and topics featured in the CRISC exam with the use of 550 questions.

Many questions have been revised or completely rewritten to be more representative of the current CRISC exam question format, and/or to provide further clarity or explanation of the correct answer. These questions are not actual exam items, but are intended to provide CRISC candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam.

Print Product Code: CRQ5ED
Member Price: $72.00
Non-member Price: $96.00
Print book available in Chinese and Spanish.

CRISC™ Review Questions, Answers & Explanations Database—12 Month Subscription

The CRISC Practice Question Database is a comprehensive 550-question pool of items that contains the questions from the CRISC Review Questions, Answers & Explanations Manual 5th Edition. Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CRISC candidates to identify their strengths and weaknesses and focus their study efforts accordingly. The database is available via the web, allowing CRISC candidates to log in at home, at work or anywhere they have Internet connectivity.

Database Product Code: XMXCR14M-12M
Member Price: $185.00
Non-member Price: $225.00
MAC and Windows compatible.


The CRISC Review Manual, 6th Edition is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities. The manual has been enhanced over the past editions and represents the most current, comprehensive, peer-reviewed IT-related business risk management resource available worldwide.

The 6th edition manual is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

- IT Risk Identification
- IT Risk Assessment
- Risk Response and Mitigation
- Risk and Control Monitoring and Reporting

The CRISC Review Manual 6th Edition offers an easy-to-navigate format. Each of the book’s four chapters has been divided into two sections for focused study. Section one of each chapter contains:

- Definitions and objectives for the four areas
- Task and knowledge statements
- Self-assessment questions, answers and explanations
- Suggested resources for further study

Print Product Code: CRR6ED
eBook Product Code: EPUB_CRR6ED
Member Price: $105.00
Non-member Price: $135.00
Print book available in Chinese, Japanese and Spanish.

The CISM® Review Manual, 15th Edition is designed to help you prepare for the CISM® exam. This comprehensive, easy-to-navigate manual is organized into chapters that correspond to the four job practice areas covered in the CISM exam. The Manual is primarily designed as a tool for exam prep, but can also be useful as a reference manual for information security managers.

New to the 15th Edition:
- **In Practice Questions** help you explore the concepts in the CISM Review Manual in your own practice.
- **Knowledge Checks** are designed to help reinforce important concepts from the Review Manual to further enhance your learning.
- **Case Studies** provide real-world scenarios to help you gain a practical perspective on the Review Manual content and how it relates to the CISM’s practice.
- **Comprehensive Index** has been updated to make navigating the Review Manual easier and more intuitive.

The CISM Review Manual 15th Edition maintains features from previous editions including:
- Task and knowledge statements
- Self-assessment questions
- Suggested resources for further reading
- Glossary


The CISM® Review Questions, Answers & Explanations Manual, 9th Edition consists of 1,000 multiple-choice study questions, answers and explanations, which are organized according to the CISM job practice domains.

The questions, answers and explanations are intended to introduce the CISM candidate to the types of questions that appear on the CISM exam. This publication is ideal to use in conjunction with the CISM Review Manual 15th Edition.

To help exam candidates maximize—and customize—their study efforts, questions are presented in the following two ways:
- Sorted by job practice area
- Scrambled as a sample exam

CISM® Review Questions, Answers & Explanations Database—12-Month Subscription

The CISM® Review Questions, Answers & Explanations Database is a comprehensive 1,000-question pool of items that contains the questions from the CISM® Review Questions, Answers & Explanations Manual 9th Edition.

The database is available via the web, allowing our CISM candidates to log in at home, at work or anywhere they have Internet connectivity.

Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CISM candidates to identify their strengths and weaknesses and focus their study efforts accordingly.
LEARN, PRACTICE AND PROVE YOUR SKILLS ONLINE WITH THE CYBERSECURITY NEXUS® (CSX) VIRTUAL CYBER ACADEMY.

The demand for professionals with technical cybersecurity skills is at an all-time high. Get the training you need, when and where you need it, with ISACA®’s Cybersecurity Nexus™ (CSX) Virtual Cyber Academy:

- Anytime, anywhere online access
- Real-world training in a live, dynamic network environment
- Comprehensive courses, hands-on practice labs, real-time assessment, and credentialing opportunities
- Learning solutions for every experience level
- Individual instructional courses and practice labs available—or save more with a full one-year subscription

TO GET STARTED, VISIT ISACA.ORG/CSX-VIRTUAL-CYBER-ACADEMY/OVERVIEW
ISACA CERTIFIED, MEANS QUALIFIED.

DISTINGUISH YOURSELF WITH GLOBALLY RECOGNIZED CERTIFICATIONS

SEE WHAT’S NEXT, NOW
Information systems and technology are constantly evolving. But, your way to get ahead in audit, security, cybersecurity, risk, privacy and governance remains the same—ISACA’s globally recognized certifications. These credentials are designed for forward-thinking professionals across a variety of industries. ISACA certifications are not just any certifications, they are the ones that can get you ahead!

REGISTER NOW FOR A 2018 EXAM
Choose your certification and exam prep that best suits your needs—get started today!

www.isaca.org/GetCertified-Jv6