MOBILE WORKFORCE 04

Social Media Rewards and Risk
Mobile Workforce Security Considerations and Privacy
Exploring How Corporate Governance Codes Address IT Governance
RECOGNIZED GLOBALLY.
IN-DEMAND LOCALLY.

REGISTER FOR AN UPCOMING ISACA® CERTIFICATION EXAM TODAY!
Secure your seat and your future—take the first step today!
1 August – 30 September 2017  |  Register today at www.isaca.org/exams2017-Jv4

What are the advantages of computer-based testing?

> More opportunities to take an exam
> Larger test center network—over 880 locations
> Faster exam results
> Test centers designed specifically for testing
> Increased flexibility for changing exam times


Take the first step towards obtaining a globally respected ISACA certification and becoming recognized as one of the most-qualified professionals in your field of information systems.

Want to see how ISACA members save?

www.isaca.org/JustASK
6th Annual European Compliance & Ethics Institute
25–28 March 2018 | Frankfurt, Germany

- Hear from top compliance & ethics professionals from Europe and around the world
- Learn the latest and best solutions for compliance & ethics challenges, including anti-corruption, data protection, and risk management
- Build your professional network
- Earn the continuing education units you need, and take the Certified Compliance & Ethics Professional - International (CCEP-I)® exam
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.

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.

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone +1.847.660.5505
Fax +1.847.253.1755
www.isaca.org
Some time ago in this space, I used an obscure statement by a nearly forgotten British Prime Minister to make some points about cyber security.1 As it happens, I studied the history of the period between the World Wars in my university days, so I often use some of the insights I gained in looking at then-current affairs when thinking about information security. I would like to turn now to a somewhat more famous artifact of the interwar years, the Maginot Line.

Here is what most people know: The Maginot Line was a series of fortifications near the French-German border intended to prevent German forces from invading France through Alsace and Lorraine, as Germany had done in two previous wars. Once those two nations entered into war again in 1939, the German forces went around the Maginot Line and invaded France once again. Thus, the term “Maginot Line” is today a catch-phrase for an expensive, foolhardy security failure.

The infamous line was named for André Maginot, a French politician who served in many cabinets in the 1920s and ’30s, three times as the Minister for War.2 Having spent much of his life in Lorraine, he was primarily concerned with protecting that part of France. He was not the visionary of the line; the idea came from the World War I French generals, particularly Marshal Henri Petain, the “hero of Verdun.”3 Neither was Maginot the leader who built the line; that was Paul Painlevé, his successor as War Minister.

So, what did André Maginot do? And what are the lessons of André Maginot and his line regarding information security generally (this is, after all, the Information Security Matters column), and cyber security specifically?

The Fallacy of Protecting Critical Resources

With the wisdom of hindsight, we know that the Maginot Line failed to protect France, but that was not André Maginot’s primary objective at the time. He and the generals before him wanted to make invasion through Alsace and Lorraine impractical, if not impossible. And it worked! France was invaded in 1940 through Belgium instead. In cyber security terms, a strategy of protecting critical data resources, with less consideration given to so-called “Tier 2,” simply exposes everything via the easiest route for an attacker to traverse. In other words, cyber security needs to treat the security of the IT environment holistically.

Moreover, it must be recognized that the methods of the cyberattackers are not monolithic and invariable. As an organization implements certain preventive measures, so those attackers intent on violating the integrity of information systems adjust their tactics. Effective antivirus filters once forced hackers to develop other forms of malware. Then, organizations became better at countering these new forms of hostile software. Now, it seems that the attackers are focusing instead on stolen credentials taken from authorized data users. This approach favors the antagonist in many ways: There is no need to find a zero-day or unpatched vulnerability, it is harder to detect, and it is more flexible once the credentials are used.4

Steven J. Ross, CISA, CISSP, 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.

Do you have something to say about this article?
Visit the Journal pages of the ISACA® website (www.isaca.org/journal), find the article and click on the Comments link to share your thoughts.

Cyber Security Must Align With the Culture

Even as the Maginot Line was being built, French generals realized that it might prove ineffective if it did not extend to the sea. But the Belgian government could not be convinced to build its own line nor would the French build one along its Belgian frontier. The political and economic environment would not permit more to be spent on preventing invasion.

There are political and economic environments within companies and government agencies that we often term the “corporate culture,” within which there is a security culture. Organizations will not, or cannot, do more for information security than that culture allows. Maginot understood that. Paraphrasing him in today’s terms, the security culture within all organizations is the best safeguard against overspending (or underspending) on cyber security. “It controls not only the purse, but the man-power of the organization.”

Moreover, it appears that Maginot recognized that no one protective measure could win a war, although it could provide an essential edge in a battle, just as no one security tool is going to solve the problem of cyberattacks. Preventive software and hardware must fit within a technology environment that includes alarms and responsive triggers, analytics and recoverability. In addition, and closer to the context of culture, these tools must be incorporated into an organizational structure of monitoring and preparedness.

Winning the Budget Battle Wins the Cyberwar

Maginot’s great achievement was to recognize the spirit of his times, the zeitgeist, and take advantage of it. In an era marked equally by fear, pacifism and unemployment, he found it easy to appeal for funding of a line of fortifications, a passive measure to strengthen defenses and create jobs at the same time. In fact, Maginot did not attempt to sell the line of fortifications as the sole or even the primary means of preventing invasion. He stated, “We could hardly dream of building a kind of Great Wall of France, which would in any case be far too costly. Instead we have foreseen a powerful but flexible means of organizing defense, based on the dual principle of taking full advantage of the terrain and establishing a continuous line of fire everywhere.”

Is any organization today prepared to build a Great Wall of IT? Even contemporary militaries do not have infinite budgets for cyberdefense (or attack, for that matter). What we are seeking is to take full advantage of organizing the preventive, detective and recoverability techniques we have in as economical a manner as possible and to establish a comprehensive program of cyber security. Budget monies are available with these wide-ranging, but nonetheless finite, goals. We may never “win” the war against cyberattacks, whatever winning means in this case. If we can gain the budget to make this war easier to fight and the risk easier to manage, that may be victory enough.
Endnotes


2 Charles River Editors, The Maginot Line: The History of the Fortifications that Failed to Protect France from Nazi Germany During World War II, USA, 2015. The historical material on André Maginot and the Maginot Line comes from several sources. This publication is a good general discussion.

3 And the traitor of Vichy.


5 WebCite, “André Maginot: A History,” www.webcitation.org/5kn33HV01

6 Ross, S.; Creating a Culture of Security, ISACA®, USA, 2011, p. 21. Will this shameless self-promotion never stop?

7 Philip, P. J.; “Death of Maginot a Loss to France,” The New York Times, 8 January 1932. What Maginot actually said, as translated by the The New York Times, was, “Public opinion in all free democracies is the best safeguard against overarmaments. It controls not only the purse but the man-power of the nation. It is only in autocratic countries in which the people [sic] are not their own masters that armies and military caste become a menace. That is what happened in Germany in 1914. If we are still unconvinced that it will happen again we must be excused. Give us, and let us give Germany, time.” In finding this quotation, I was amazed at how much Maginot’s views from the early 1930s resound today.

It was a great compliment, if somewhat daunting, to be invited to follow in the footsteps of Tommie Singleton and the late Ed Gelbstein to contribute to this column. I can only hope to match their insights by bringing my own experiences to bear.

Speaking of which, one of the most common requests I get as a community leader on the ISACA® Knowledge Center1, 2, 3 is for audit/assurance programs or sources of assurance. So, what are our options and where should we look?

**Utilize Existing Audit/Assurance Programs**

ISACA, the Institute of Internal Auditors (IIA) and other organizations have developed programs (figure 1) that address commonly audited areas such as cyber security, commonly utilized applications such as SAP and common requirements for compliance such as the Payment Card Industry Data Security Standard (PCI DSS). These are excellent resources and can save a lot of time. My only word of warning is that they are not one size fits all. They should be considered a starting point and adjusted based upon risk factors and criteria that are relevant to the organization you are auditing. Failure to do so can result in a checklist approach that can lead to the auditor recommending controls that are not applicable to the organization. This, in turn, can damage your reputation with the auditee and, ultimately, with senior management.

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA</td>
<td>Audit/assurance programs4</td>
</tr>
<tr>
<td>IIA</td>
<td>Global Technology Audit Guides (GTAGs)5</td>
</tr>
<tr>
<td>AuditNet</td>
<td>Audit Programs6</td>
</tr>
</tbody>
</table>

Source: Ian Cooke. Reprinted with permission.

**Build Your Own**

During your career as an IS auditor, there will be a requirement to build your own audit/assurance programs. These would typically be required when the audit subject is a custom-built application or when the organization being audited is implementing tools or processes that are on the cutting edge. How do you approach such assignments?

In March 2016, ISACA released an excellent white paper titled *Information Systems Auditing: Tools and Techniques Creating Audit Programs.*7 The paper describes the five steps in developing your own audit program (figure 2). Essentially, these steps are:

1. **Determine audit subject**—What are you auditing? This is often set as part of the overall audit plan.
2. **Define audit objective**—Why are you auditing it? Again, this may have been set as part of the overall audit plan.
3. **Set audit scope**—What are the limits to your audit?
4. **Perform preaudit planning**—What are the specific risk factors?
5. **Determine audit procedures and steps for data gathering**—How will you test the controls for these risk?

A crucial component of step 5 is developing the criteria for evaluating tests. "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.\(^9\) Many of these will be defined by the entity that is being audited (e.g., contracts, service level agreements, policies, standards); however, there will be instances, for example, when an organization has not defined its own standards when other criteria should be applied (figure 3).

One such instance might be when you are auditing an Oracle database. Where an organization has defined its own Oracle database standard, then you audit to that standard. However, if no standard exists, it is good practice to use an external benchmark if it is objective, complete, relevant, measurable, understandable, widely recognized, authoritative and understood by, or available to, all readers and users of the report.\(^9\) Further, IS audit

---

**Figure 2—Creating an Audit Program**

1. **Determine audit subject.** Identify the area to be audited (e.g., business function, system, physical location).
2. **Define audit objective.** Identify the purpose of the audit. For example, an objective might be to determine whether program source code changes occur in a well-defined and controlled environment.
3. **Set audit scope.** Identify the specific systems, function or unit of the organization to be included in the review. For example, in the previous example (program changes), the scope statement might limit the review to a single application, system or a limited period of time.
4. **Perform preaudit planning.**
   - Conduct a risk assessment, which is critical in setting the final scope of a risk-based audit. For other types of audits (e.g., compliance), conducting a risk assessment is a good practice because the results can help the IS audit team to justify the engagement and further refine the scope and preplanning focus.
   - Interview the auditee to inquire about activities or area of concern that should be included in the scope of the engagement.
   - Identify regulatory compliance requirements.
   - Once the subject, objective and scope are defined, the audit team can identify the resources that will be needed to perform the audit work.
5. **Determine steps for data gathering.** At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit program. Some of the specific activities in this step are:
   - Identify and obtain departmental policies, standards and guidelines for review.
   - Identify any regulatory compliance requirements.
   - Identify a list of individuals to interview.
   - Identify methods (including tools) to perform the evaluation.
   - Develop audit tools and methodology to test and verify controls.
   - Develop test scripts.
   - Identify criteria for evaluating the test.
   - Define a methodology to evaluate that the test and its results are accurate (and repeatable if necessary).
and assurance professionals should consider the source of the criteria and focus on those issued by relevant authoritative bodies before accepting lesser-known criteria.\(^{23}\) I would also disclose the criteria used and why—in this case, auditors were required to give an opinion on the security of an Oracle database, but management had no standard defining what “secure” means. A further finding from such an audit may be that management should define such a standard. Selecting the right criteria is vital for the success of the audit.

**Collaborate**

We live in a world where it is very much a viable option to run a business using open-source software. I, therefore, pose a simple question: Why cannot we, as an ISACA community, develop open-source audit/assurance programs?

The Documents and Publications section of Audit Tools and Techniques\(^ {24}\) allows every member to contribute user-created documents and publications. Members could, therefore (with their organization’s permission), upload completed audit/assurance programs, making them available (with the right terms and conditions) for other members to adopt for their own enterprise’s risk and criteria. Further, other members could contribute to and enhance these documents. Over time, we, as a community, could build up many audit/assurance programs that are continuously enhanced and kept up to date.

**Conclusion**

An audit/assurance program is defined by ISACA as a step-by-step set of audit procedures and instructions that should be performed to complete an audit.\(^ {25}\) Many of these steps are common to most enterprises; however, each also has its own culture, ethics and behavior. We can utilize and share existing audit/assurance programs and even

---

**Figure 3—Sources of Assurance/Good Practice**

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA</td>
<td>COBIT 5(^ {12}) White papers(^ {11}) Cloud computing guidance(^ {12}) Cyber security resources(^ {13})</td>
</tr>
<tr>
<td>US Department of Defense</td>
<td>Security Technical Implementation Guides (STIGs)(^ {14})</td>
</tr>
<tr>
<td>ISO</td>
<td>Center for Internet Security Benchmarks(^ {15})</td>
</tr>
<tr>
<td>CSA</td>
<td>Cloud Security Alliance(^ {17})</td>
</tr>
<tr>
<td>NIST</td>
<td>US National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity(^ {18}) Security and Privacy Controls for Federal Information Systems and Organizations(^ {19}) NIST publications(^ {20})</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard(^ {21})</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information Technology Infrastructure Library(^ {22})</td>
</tr>
</tbody>
</table>

*ISO and PCI DSS can also be used as sources of best practice even where compliance is not required.

Source: Ian Cooke. Reprinted with permission.

---

> **Why cannot we, as an ISACA community, develop open-source audit/assurance programs?**
collaborate on the building of same if we remember that we have an obligation to consider the risk to our own organizations.

**Editor's Note**

ISACA is currently exploring several methods for community-driven audit program sharing and development models.

**Endnotes**

1. ISACA® Knowledge Center, Audit Tools and Techniques, www.isaca.org/it-audit-tools-and-techniques
2. ISACA Knowledge Center, Oracle Databases, www.isaca.org/topic-oracle-database
4. ISACA, Audit/Assurance Programs, www.isaca.org/auditprograms
6. AuditNet, Audit Programs, www.auditnet.org/audit_programs
9. Op cit, ITAF, p. 20
22. Information Technology Infrastructure Library, https://www.itil.org.uk/all.htm
23. Op cit, ITAF, p. 20
24. Op cit, ISACA Knowledge Center
Q: As ISACA's incoming chair of the Board of Directors, how do you see ISACA® growing and adapting to the constantly changing marketplace and needs of its constituents over the next year?

A: New technologies—and threats—are introduced almost daily. ISACA represents an interrelated, yet diverse, set of constituents. As risk, audit, security, cyber and governance professionals, we need to be agile and prepared. Whether it is through partnering with other professional associations on content development or training, or the way in which it structures its volunteer committees, ISACA is looking at ways to become more agile to better serve its members and their professions. For example, ISACA was once tied to a volunteer structure that allowed appointments and changes on only an annual basis. By moving to a more agile model, ISACA is now able to move from a reactive to a proactive posture to tackle changes in technology, threats and future trends.

Q: Can you briefly describe your role as inspector general (IG) of the US House of Representatives? What in your past experience has best prepared you for this position?

A: As IG of the US House of Representatives, I am a nonpartisan, senior House official who is jointly appointed by the speaker, majority leader and minority leader of the House. I am responsible for planning and leading independent audits, advisories and investigations of the financial and administrative functions of the House. Aside from having the necessary technical skills, I believe the experience that most prepared me for this position is, oddly, a moral philosophy class that I took as an undergraduate at St. Joseph's University (Philadelphia, Pennsylvania, USA). Father Lombardi stressed that to really understand what you believe in, you need to understand a problem from all sides—and be able to argue with equal strength from all sides. As a person who needs to get bipartisan approval on everything I do, understanding how people think, how they solve problems and how they prioritize things has been critical in tackling important issues, bridging divides and, ultimately, making a difference.

Q: How do you believe the certifications you have attained have advanced or enhanced your career? What certifications do you look for when recruiting new members to your professional team?

A: I believe getting certifications has proven my commitment to my profession and to lifelong learning. Certifications are an outward representation and assurance of your skills, but they represent only one aspect of professional commitment. Getting involved and participating in a professional association demonstrates your connection to the

Theresa Grafenstine, CISA, CRISC, CGEIT, CGAP, CIA, CISSP, CPA is chair of ISACA®'s Board of Directors and the inspector general (IG) of the US House of Representatives (House). Over the past 25 years, Grafenstine has served in the IG community in both the legislative and executive branches of the US federal government. As the IG, she is responsible for planning and leading independent, nonpartisan audits, advisories, and investigations of the financial and administrative functions of the House. Prior to joining the US House Office of Inspector General (OIG), Grafenstine served at the US Department of Defense OIG where she led acquisition audits of major weapon systems and was selected to respond to high-profile US Congress audit requests. She is a past chair of ISACA’s Audit Committee, Finance Committee, Communities Committee, and Relations Board and a past president of the ISACA National Capital Area Chapter. Grafenstine also serves on the board of directors of the Association of International Certified Professional Accountants (AICPA) and as the audit committee chair of the Pentagon Federal Credit Union. She has received numerous awards and accolades, including the Golden Gov: Federal Executive of the Year and, most recently, the Greater Washington Society of CPAs 2016 Women to Watch and 2016 Outstanding CPA in Government awards.
broader professional community and helps you grow as an industry leader. When hiring staff at the House, I look for diverse certifications and higher degrees to help address the broad range of problems we face. Even as a senior executive, I like to show my commitment to the profession and prove my capability to my staff (and to myself!) by sometimes sitting for the same training and exams they are pursuing—which is the reason why I have so many certifications!

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

A: I think an ongoing challenge for any professional is the rapid pace of change. How do we keep up with it? How do I find and retain staff who can meet the changing demands? This is even more so in the congressional environment. Every member of the House of Representatives is up for reelection every two years. In addition to the changes brought about by elections, leadership positions change as well.

In my seven years as IG, I have served under three different Speakers of the House and four different congressional oversight committee chairmen. With all of these changes in leadership come changes in priorities, focus and direction. It teaches you to be nimble in adjusting the audit plan. You also need to be able to quickly acquire new or different skills to adjust to the changing priorities. That agility has made me a better auditor and a better leader because it forces me to constantly think on my feet and help others, who may struggle with change, to adapt.

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

A: Diversity goes beyond a feel-good social initiative; it impacts the bottom line. It is a powerful resource that, if properly leveraged, increases an organization’s ability to connect with a broader base of people, deepens an organization’s knowledge base and, ultimately, reduces enterprise risk. When there is a pipeline shortage of women to fill senior leadership roles or in science, technology, engineering and mathematics (STEM) career fields in general, this puts organizations at risk. Women leaders bear a special responsibility to help fill this pipeline by serving as role models and mentors to our next generation of leaders. We need to connect with girls and young women to show them what a Woman in Technology leader looks like. If we wait until they have already made career decisions, it may be too late. I think it is important to volunteer at local schools as speakers on career day. I think it is especially important to reach out to schools in at-risk communities to show students that IT security is an amazing career option. If they have never heard of it, they cannot choose it. We can not only address some of the pipeline issues, but we can literally change the trajectory of young people’s lives.

Q: What is the biggest security challenge that will be faced in 2017? How should it be addressed?

A: The biggest challenge, is the human element. Lack of employee cyberawareness, weak passwords, failure to implement patches, falling for phishing scams and insider threat will do more cumulative damage than complex emerging issues.

Q: What are your three goals for 2017?

A: 
- Developing a leadership pipeline
- Continuing and strengthening ISACAs Women in Technology initiative
- Exploring charitable options through ISACA’s ITGI foundation to give opportunities to people in developing nations or underrepresented demographics to obtain leadership skills, relevant training and certifications.

Q: What is your favorite blog?

A: ISACA International does a great ISACA Now blog. CyberScoop and NextGov do a great job of reporting on important issues.

Q: What is your number-one piece of advice for other audit professionals?

A: Do not rest on the fact that you are a regulatory requirement. Provide value to your organization every day.

Q: What is your favorite benefit of your ISACA membership?

A: The fantastic people—the members, the volunteer leaders and the staff. ISACA has benefited my career in monumental ways, but the biggest benefit has been the friendships.

Q: What do you do when you are not at work?

A: When I am not at work and I am not doing ISACA work, I am at my son’s ice hockey game, helping my daughter find the right college or walking the dogs with my husband.
Enterprises worldwide need qualified cyber professionals to fill the gap in their cyber security capabilities. Eight in ten organizations would be more likely to hire a candidate with a performance-based certification.*

The intensive, 5-day **CSX Accelerated Cybersecurity Skills Training** from ISACA’s Cybersecurity Nexus™ (CSX) will elevate your skills to the level of an experienced, in-demand cyber security first responder — and prep you for the SC Magazine award-winning **CSX Practitioner Certification** — at the pace you need for success.

Join us for our next course:
• Chicago, Illinois: 31 July – 4 August 2017

Seats are limited. Act now to secure this invaluable training. Visit CSXPTraining.com to learn more.

---

*ISACA’s January 2016 Cybersecurity Snapshot survey.

†CSX Practitioner is the 2016 SC Magazine Award Winner for Best Professional Certification Program.
Social Media Rewards and Risk

Mohammed J. Khan, CISA, CRISC, CIPM

Social media is a powerful tool that gives organizations the ability to expand their brand value; it can also tarnish a brand overnight. There are more than 18 social media platforms globally that have started to grow and have an enterprise-level following, and this is only the beginning. Given the visibility, risk, and real-time monitoring and response required to effectively manage social media channels, companies must establish extensive protocols for use by their organization in order to engage with external channels. Companies representing themselves externally should engage the appropriate and authorized spokespersons and executives designated by their communications department in order to speak to, initiate, provide and/or post information within the social media space. While there are several key risk factors to be addressed relative to social media, there are many rewards as well. Some of the most advanced topics and benefits include (figure 1):

• Connecting with customers—The ability to engage with customers is the most critical aspect of social media. Developing a brand and promoting it through various channels of social media can create further brand value and awareness.

• Marketing intelligence—Social media marketing gives the organization the ability to monitor the brand and listen to what the public is saying in the social media space. The insight is the reward the organization reaps by playing a larger role in social media, which can be invaluable. The organization can enhance its marketing, business development efforts and other valuable venues to further its ability to be competitive.

• Pulse on brand reputation—Keeping the pulse of the organization’s social media reputation and metrics is critical to staying ahead of the brand’s recognition and signs of reputational risk.

As for the risk (figure 2), some of the most common ones include:

• Reputational risk—Damage to an organization’s reputation stemming from a social media mishap can bring the organization to its knees, whether it is the chief executive officer (CEO) stating something controversial on his/her Twitter account or an organization-bashing employee video that goes viral. According to a leading publisher, “A reputational crisis can wipe tens of millions of pounds from a company’s value, and this risk has increased because the rise of online and social media means crises are now less predictable and can happen faster.”

• Data security breach—According to research from Forrester:

  From reconnaissance to brand hijacking and threat coordination, cyber criminals have been using social media to boost the effectiveness of their attacks for years. It’s clear that social media risk isn’t solely about brand and reputation damage but is a sinister cybersecurity threat that can lead to major data breaches, numerous compliance issues, and large amounts of lost revenue due to fraud and counterfeit sales, along with a slew of other risks.

• Social engineering—Employees in almost all organizations are savvy, and many have a social media presence on major sites such as Facebook, LinkedIn, Quora and Twitter. Each platform has

Mohammed J. Khan, CISA, CRISC, CIPM

Is a global audit manager at Baxter International, a global medical device and health care company. He has more than 12 years of experience focused on providing privacy, security and information governance. Most recently, he has focused specifically on medical device cyber security, global privacy frameworks, and helping his organization with strategic, cost-effective initiatives in the audit and compliance space. Khan previously worked for a leading consultancy firm as an assurance and advisory professional, and prior to that, he worked as a global enterprise resource planning and business intelligence professional at a leading technology firm. Khan has helped develop and author several publications and has presented at industry conference events focusing on privacy and cyber security.
Figure 1—Organizational Benefits of Social Media

**Reward 1**
- **Connect**
  - Engage with customers
  - Develop promotional material with industry consortium
  - Build brand awareness

**Reward 2**
- **Intelligence**
  - Insight into competitors’ market
  - Relevance in the marketplace

**Reward 3**
- **Reputation**
  - Pulse on brands’ integrity in the social media space

Source: M. Khan. Reprinted with permission.
Employees who access social media websites can act as brand ambassadors; on the other hand, their activity may leave an open door for viruses and malware to enter into the network.

• **Compliance to changing the regulatory climate**—These regulatory changes require the organization to adapt its strategy if it wishes to comply on a global basis. This approach, while necessary for an organization that uses social media regularly, may result in the organization’s increased visibility with authorities.

Some industries may shy away from this situation in light of audits that occur due to being in the social media space so frequently.

• **Return on investment**—The benefit the organization gains from being present in the social media space is hard to calculate and very subjective. The risk over reward, therefore, cannot be calculated without proper assurance, which leaves the decision to enter the social media space questionable for some industries.

• **Phishing**—One of the popular techniques used by criminals is to get unknowing individuals to disclose personal information while posing the potential to provide a hacker several key data points about employees, which can enable use of the data to hack the employee account at the enterprise layer by spoofing and launching a social engineering attack on the company. Due to the multitude of options of going through social media accounts with exposed data, attackers can gather these data to further their advances in terms of hacking into accounts.

**Compliance or regulatory violations**—The growing number of privacy changes and regulations globally is impacting how customer data are utilized in the social media space. There are four key areas with which to be concerned:

- Privacy
- Content ownership
- Intellectual property (IP) infringement
- Unauthorized activities
as a fictitious representative of a legitimate professional or company. This, primarily, is the key driver for collecting personal data for financial gain to individuals or organizations. Due to the lack of awareness about the phishing techniques used by hackers, employees fall victim to email, phone call and website phishing schemes, resulting in exposure to enterprise-level risk.

• Viruses and malware—Hackers’ ability to penetrate the organization’s network via unsafe social media websites and accounts opens a new threat vector. On one hand, employees who access social media websites can act as brand ambassadors; on the other hand, their activity may leave an open door for viruses and malware to enter into the network. According to security experts, “A majority of current attacks simply use the social platforms as a delivery mechanism, and have been modeled after the older Koobface malware.”

Preventing Social Media Risk

Some organizations struggle to develop the best solution to manage risk around social media. The first question to ask is who, in fact, owns the social media platforms for the organization and, more importantly, the overall governance of the social media of employees. Social media impacts all departments of the organization, and each department, whether it is IT, finance, marketing or human resources (HR), has a different perspective of how social media can or will be utilized by the department on behalf of the organization. There is no prescribed rulebook for eliminating social media risk to an enterprise; however, some key areas to consider for preventing social media risk are:

• **Guidelines**—As general best practice, a high-level overall policy should be rolled out to guide the use of social media by all employees of the organization and any third party acting on behalf of the organization. The guidelines should highlight key components including:
  – **Scope**—Defining the overall scope of the policy guidelines that is set forth by the enterprise for its employees
  – **Purpose**—Definition of the purpose of the guidelines for the organization, specifically, how social media activity on behalf of the organization will take place and what sort of information is relevant to share via that activity
  – **Goals**—Clear definition of the overall outcome that is to be achieved from the social media presence for the organization and how the social media platform will get the organization there
  – **Ownership guidelines**—General guidelines for the creation and maintenance of all social media sites for the organization

“**A robust social media crisis and communication plan must be developed in the event that a crisis occurs.**”
Conclusion

Organizations that plan to increase or decrease their presence on social media would be well advised to exercise awareness and vigilance. Different industries may experience various benefits and disadvantages to jumping on the social media bandwagon. Organizations planning to engage on social media platforms must have a clearly defined policy and communication plan in place. Proper considerations should be made for good governance, a communication plan in the event of a breach, a social media policy and monitoring tools, which are all important for enterprise-level social media risk mitigation.

Deciding which social media channels to use and performing due diligence and evolutionary management of the social media space the organization enters are critical. The first step is to understand the benefits and the disadvantages while keeping in mind the basic steps that can be taken to mitigate risk.

Endnotes

Mobile Workforce Security Considerations and Privacy

In 2012, a software developer who mainly worked remotely for a US firm had the idea of fully outsourcing his work to China. He was finally caught after a few months because of suspicions about the origination of his virtual private network (VPN) connections. Indeed, he literally sent his physical VPN key access to his remote “employee” to allow him to access the company’s systems. Although this story might appear to some extent anecdotal, it raises some serious issues about security considerations and even privacy around remote working and what it entails. How is it possible that an employee gave unauthorized access to his company information to an outsider for so long without it being noticed? What are the legal and reputational consequences for the company? Are the connections of employees always monitored, and what are the employer’s intentions when monitoring them?

Remote working has a lot of advantages, both for the company and the employees. In the past years, it has become increasingly used by companies as a perk. In some countries such as the UK, it is even an employee right to request mobile working. The desire for mobility comes from the sense of flexibility, liberty and self-management it entails, especially for those who need to watch over their children and/or have a long commuting time to reach their physical office location. It also gives a sense of job ownership to the employees, although it often adds a “hidden” pressure on them. For example, remote employees do not want their management to think that if they are not delivering as expected it is because working remotely is holding them back; therefore, they will work even more than the contractual hours to deliver. It also helps companies cut costs, especially in rent and utilities, and find skilled employees regardless of their location. With the progress of technology, the mobile workforce is a trend that is not going to stop and will even expand. It is forecasted that by 2020, 72.3 percent of the US workforce will be remote.

It is also clear that this modern workforce comes with risk, which can be substantial if not properly addressed.

Mobile Workforce and Technology

Technology enables the mobile workforce. In recent years, many technology companies such as Google, Amazon and IBM have started to invest massively to offer cloud-based services to respond to businesses’ expectations. Beyond being willing to promote workforce mobility, an investment should be made in technology to effectively implement it.

With the development and continuous improvement of cloud technologies, it is now very easy to bring almost all the tools used at the physical workplace to employees’ homes and even to their smartphones. In many companies, employees are even allowed to use their own devices and install security systems to secure information.

There are also many companies providing various tools for videoconferencing, conference calls and document sharing such as Skype, Webex and Google Hangout, that enable connection and collaboration among employees and with customers. One recent major example of investment in cloud-based technology is PricewaterhouseCoopers’s (PwC’s) partnership with Google to switch to collaborative tools in order to stay at the forefront of the technology and use the full opportunity that mobile workforce offers. According to a survey conducted by PwC, 77 percent of chief executive officers (CEOs) believe that technologies are a top value driver for...
secured, or they could choose to work in public area like cafes, parks or bus stops. Of course, this causes serious threats, not only to data integrity, but also to the physical security of employees. These threats are more easily mitigated when working in a physical office because there are plenty of countermeasures companies have been implementing for decades.

While the negligence of remote employees can be one major source of risk related to the company’s assets, there is also risk related to cloud technology. The key areas of risk to consider when it comes to a mobile workforce follow.

**Company Assets**
The biggest risk in this area is loss or damage to the assets when they are in possession of the remote employees. These assets can be physical (laptops, mobile phones, tablets) or logical (customers’ data, employees’ data, other critical information). Threats can range from a child pouring water on a laptop to a device shared within the employee’s family without appropriate safeguards to a computer screen inadvertently left unlocked while displaying sensitive information. There are many situations that...
can lead to the impairment of assets. In a simple example, Kendi, who is an employee of ABC, has an important call to discuss confidential information. She decides to make the call from her garden and her neighbor and even one of her guests is listening to the conversation. In the worst-case scenario, Kendi’s part of the conversation is recorded and that information disclosed to the general public. The consequences could be catastrophic for her firm, its clients and even herself.

Also, hackers or other individuals or organizations willing to steal data from a company can take advantage of remote workers to accomplish their tasks knowing they are more likely to succeed by attacking one isolated employee than breaking the security layers of an entire organization.

Personal Security
Employees who are carrying or storing important assets of companies at home are at increased risk of being attacked to take control of the asset. It can be a single robber who is willing to steal a mobile phone and resell it without any knowledge of the contents, or it can be a more organized criminal group that is fully aware of the value of the data in the employee’s possession.

This is particularly true for workers who consistently work at home because the level of home security is unlikely to be as rigorous as at an office building, and criminals realize, from the worker’s regular, daily routine, that they can take time to plan their activities and, therefore, increase their likelihood of succeeding.

Cloud Technologies
Whether a company partially or totally outsources its systems and infrastructures, typical IT risk related to confidentiality, integrity and availability around IT governance and management, access to programs and data, change management, and operations still holds. In addition to the risk that usually exists in an office environment, the risk arising from Internet use and all that entails increases significantly. Indeed, because cloud providers have many customers, the information they store and manage has great value for hackers, who will try to take advantage of Internet use to find breaches into the information system and gain access to the data.

It is critical for companies to be aware that cloud providers have their own employees who can access companies’ data (thereby customers’ data) and steal that data for various purposes.

Regulation and Compliance
Depending on their activities, companies are required to comply with various laws and regulations regarding their information systems and the data they manipulate. These regulations differ from one country to another. In the US, health care data security is chiefly governed by the US Health Insurance Portability and Accountability Act (HIPAA), while in the UK there are the National Health Service (NHS) Act of 2006, the Health and Social Care Act of 2012, and the Data Protection Act.

Companies need to be extremely careful about regulations with which all the stakeholders involved in mobile working must abide. In general, companies are liable for the security of their information systems, regardless of whether or not they outsource their IT. It is the company’s responsibility to ensure that customers’ data remain confidential and accurate. If the cloud vendor or a remote worker is located in a region or country
where data protection is not stringent, the data could potentially be at risk.

**Privacy Concerns**

When setting up policies relating to the mobile workforce, companies may take actions that can be viewed as privacy breaches for employees. Some companies monitor all activities (including communication) and files on devices given to the employees and even track their location. Of course, if there is no mandatory regulation that protects employees’ privacy, there can be abuses that can have tragic consequences.

Companies will always promote the benefits of monitoring their devices for security or business reasons, but employees need to be aware of privacy concerns and ensure that their personal life and information will not be impacted. According to a survey conducted by MobileIron, 30 percent of mobile employees are ready to quit their company if their devices are monitored.ª

Working remotely can often affect or expose your family. Recently, the children of Professor Robert Kelly walked into his office during his television interview with the BBC, followed by his wife, who was trying to pull them out of sight. That video was viewed millions of time on social media networks, and his family became public.

**Recommendations**

There are several measures companies can take to protect their assets and resources. The first is to clearly identify and document all potential security and privacy risk areas that relate to mobile working. It will help the company to structure its response to those risk areas and find appropriate measures. Some typical responses that can be implemented follow.

**Security and Privacy Policies**

Appropriate policies and related procedures should be defined to give clear directions on how assets and resources should be used remotely to guarantee their security. The acceptable use policy should clearly state what remote employees can or cannot do with the assets of the company, placing particular emphasis on personal use.

Human resources policies have to be clear on privacy issues, so those policies should clearly define the boundaries within which monitoring and (potentially) tracking will be performed and how employees’ privacy is protected by the company. Companies should make sure that their employees are aware of those policies and have given their consent. These policies should be enforced and monitored by an independent function, and employees should have a dedicated person or team to speak to if they feel that their privacy is not respected.

> Actively involving employees in defining and monitoring the security of company assets gives them a better sense of ownership and increases compliance to the security policies.

**Training and Awareness Programs**

One of the most effective ways to secure company assets is to offer regular training and awareness campaigns. These events should describe the risk associated with information systems used...
In relation to the last item, the vendor should be able to produce a third-party assurance report, signed by an independent auditor, which shows the status of its internal security control. Of course, the provider’s system of internal control should always be in addition to the controls managed and operated by the company itself. It is worth noting that just receiving the report is not sufficient; companies need to analyze it in detail and ensure that the level of security is appropriate to their business.

Secure Remote Communications
Remote communication is definitely one of the key areas to look at carefully with regard to mobile working. The company’s systems are not only accessed from its offices, but also from unknown locations that can present their own risk and weaknesses. To avoid, or at least to significantly decrease, the risk of intrusion into company systems, continuous network monitoring should be performed using the most advanced and up-to-date technology the company can afford.

In addition, critical communications between devices and the company’s servers should be encrypted. Employees should regularly be made aware to avoid using public Wi-Fi, unless appropriate security measures (e.g., VPN connection) have been implemented.

Secure Devices and Their Content
If a device is lost, intruders can easily get access if it has not been properly secured. Therefore, critical data should be encrypted, and strong password and session security configuration should be enforced. The screen lockdown after a period of inactivity should be set to a low value. Antivirus software should be regularly updated using a “push” method, and devices whose antivirus software is not up to date must be restricted from connecting remotely to critical systems.

From a physical perspective, computer locks can be given to employees so they can physically lock their computer when they are away from it. On mobile phones or tablets, device management

Critical data should be encrypted, and strong password and session security configuration should be enforced.

Insurance
If customers’ data are disclosed, financial damage can be significant. By taking out an insurance policy against loss or damage of assets, companies can protect themselves against such costs. Of course, the insurance premium can potentially rise due to the increased risk arising from remote working.

Monitoring Cloud Providers
The choice of cloud provider is the key decision companies must make once they commit to using cloud services. The provider must be appropriate not only in terms of cost, but also with regard to reputation, compliance with regulations and evidence of a strong control culture.
applications and suites such as Good or MobileIron can help secure business data.

Endnotes
4 Archer, T.; M. Daigle; “PwC and Google for Work,” https://gsuite.google.co.uk/intl/en_uk/learn-more/pwc_and_google_bringing_transformation_to_work.html
Exploring How Corporate Governance Codes Address IT Governance

Introduction

IT governance, also referred to as governance of enterprise IT (GEIT) or corporate governance of IT, is a subset of corporate governance that is concerned with enterprise IT assets. In an analogy to corporate governance, IT governance is concerned with the oversight of IT assets, their contribution to business value and the mitigation of IT-related risk. A commonly referenced definition states:

> Enterprise governance of IT is an integral part of corporate governance exercised by the board and addresses the definition and implementation of processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments.

Prior studies identify five domains that warrant oversight of the board of directors (BoD) and executive management in governing IT assets:

- **Strategic alignment**—Focuses on aligning business and IT strategies and operations
- **Value delivery**—Concentrates on optimizing expenses and proving the value of IT
- **Risk management**—Addresses the IT-related business risk
- **Resource management**—Optimizes IT-related knowledge and resources
- **Performance measurement**—Monitors IT-enabled investment and service delivery

Emerging research calls for more board-level engagement in IT governance and identifies serious consequences for enterprises if the board is not involved. For example, high levels of board engagement in IT governance, regardless of existing IT needs, increases enterprise performance. From the board perspective, there is also a growing need to comply with an increasing amount of regulatory and legal requirements (e.g., privacy), of which many also impact IT. These
regulatory requirements redefine the responsibilities of the BoD for IT governance.8

Despite the agreement between researchers and practitioners on the need for board-level involvement in IT governance, it appears that this is more the exception than the rule in practice.9, 10, 11 This article builds on the assumption that the behavior of the board toward IT governance and digital leadership can be influenced by external factors, such as corporate governance codes,12 and describes the study that answers the questions:

- What IT governance-related guidelines are contained in national corporate governance codes?
- What differences can be observed between various corporate governance codes?

Research Design

The research began with a literature review to underpin the study and to define the main concepts that were used in the research project.

Next, a sample of international corporate governance codes was analyzed. The selection of national corporate governance codes was based on two dimensions—geography (i.e., continent) and economy (i.e., income groups). Using an index of all of the corporate governance codes around the world,13 a national corporate governance code was selected to populate as many cells as possible (figure 1). When a country had multiple corporate governance codes, the most recent code for listed companies was selected. An additional requirement was that the corporate governance code should be available in English. The final sample of national corporate governance codes (N=15) is presented in figure 1.

![Figure 1—Final Sample of National Corporate Governance Codes by Continent and Income Group (N=15)](image)

To analyze each corporate governance code for IT-governance-related content, an IT governance transparency framework was used. This IT governance disclosure framework contains 39 disclosure items that are distributed over the following domains (focus areas): IT strategic alignment, IT value delivery, IT risk management and IT performance measurement (figure 2). Because the IT resource management domain overlays all other focus areas, the framework incorporates IT resource items across all of the four remaining IT governance focus areas. Using the

<table>
<thead>
<tr>
<th>Country</th>
<th>Code Info</th>
<th>IT Strategic Alignment (ITSA)</th>
<th>IT Value Delivery (ITVD)</th>
<th>IT Risk Management (ITRM)</th>
<th>IT Performance Measurement (ITPM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seychelles (SC)</td>
<td>2010</td>
<td>44</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>South Africa (ZA)</td>
<td>2009</td>
<td>66</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ghana (GH)</td>
<td>2010</td>
<td>27</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Japan (JP)</td>
<td>2015</td>
<td>44</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Lebanon (LB)</td>
<td>2010</td>
<td>28</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>India (IN)</td>
<td>2009</td>
<td>24</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Belgium (BE)</td>
<td>2009</td>
<td>42</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Macedonia (MK)</td>
<td>2006</td>
<td>26</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Armenia (AM)</td>
<td>2010</td>
<td>18</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Australia (AU)</td>
<td>2014</td>
<td>44</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Fiji (FJ)</td>
<td>2008</td>
<td>16</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>United States (US)</td>
<td>2013</td>
<td>27</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mexico (MX)</td>
<td>2010</td>
<td>42</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Brazil (BR)</td>
<td>2009</td>
<td>74</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Guyana (GY)</td>
<td>2011</td>
<td>16</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

IT governance transparency framework as a coding frame, a binary classification approach was used to analyze the national corporate governance codes, i.e., an item is scored 1 if the item is present as a guideline or practice in the corporate governance code and scored 0 otherwise.

**Corporate Governance Codes Make Little Reference to IT Governance or Digital Leadership**

Figure 2 presents the item-level analysis of the 15 corporate governance codes for IT governance-related content. A first general observation is that, aside from the South African code, the corporate governance codes score very low overall for including IT-governance-related practices or guidelines. A reasonable explanation is that many national corporate governance codes are based on the Organization for Economic Cooperation and Development (OECD) principles of corporate governance.17 Eight of the 15 national corporate governance codes explicitly state that they are based on the OECD principles. The remaining seven corporate governance codes show a lot of similarities with the OECD principles, but do not explicitly refer to OECD. Because the G20/OECD principles do not include specific directives regarding IT governance or IT-governance disclosure (aside from using the company website as a disclosure channel for material company information), it is not an unreasonable assumption that this might lead to a low attention to IT-governance-related matters in the national corporate governance codes that use these principles as a blueprint.

An interesting observation at the item level is that use of IT for regulation and compliance in the IT risk management domain is found in 11 of the 15 selected corporate governance codes. Again, a reasonable explanation can be found in the G20/OECD principles on corporate governance. As part of disclosure and transparency, it states that the organization website provides an excellent means to disclose material company information.18 This is, indeed, a way of using IT for regulation and compliance. Finally, the IT is part of audit committee item, belonging to the IT strategic alignment domain, is also found in the Macedonia corporate governance code. These are the only two disclosure items that were found in corporate governance codes other than South Africa.

Indeed, the South Africa corporate governance code, King III,19 contains a significant amount of IT-governance-related guidance. King III came into effect for South African entities beginning 1 March 2010 and is applicable to all entities (regardless of their size and whether or not they are listed). King III contains an IT-governance chapter consisting of seven IT-governance principles and some additional and more detailed recommended practices for each of these principles (figure 3).20

**Conclusions and Implications**

In this research project, a selection of national corporate governance codes was analyzed for IT governance-related content. The findings showed that only the contemporary South African corporate governance code, King III, contains a significant amount of IT governance-related guidance.

As IT becomes more pervasive in firms all over the world, it makes sense for boards to take on accountability for IT-related matters. This view is shared by researchers and practitioners alike. In transitioning from COBIT® 4.1 to COBIT® 5, ISACA® clearly emphasized the need for board involvement in enterprise governance and management of IT. It did so by explicitly including board-level accountabilities and responsibilities in the EDM domain, thereby further emphasizing the separation between the governance and management of IT. Because boards around the world are directly influenced by corporate governance codes, it makes sense for the committees that are drafting national corporate governance codes to include guidance for board members, to enable them for their accountabilities and responsibilities in the realm of IT governance.
<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
<th>Recommended Practices</th>
</tr>
</thead>
</table>
| 5.1       | The board should be responsible for information technology governance. | • 5.1.1. The board should assume the responsibility for the governance of IT and place it on the board agenda.  
• 5.1.2. The board should ensure that an IT charter and policies are established and implemented.  
• 5.1.3. The board should ensure promotion of an ethical IT governance culture and awareness of a common IT language.  
• 5.1.4. The board should ensure that an IT internal control framework is adopted and implemented.  
• 5.1.5. The board should receive independent assurance on the effectiveness of the IT internal controls. |
| 5.2       | IT should be aligned with the performance and sustainability objectives of the entity. | • 5.2.1. The board should ensure that the IT strategy is integrated with the company’s strategic and business processes.  
• 5.2.2. The board should ensure that there is a process in place to identify and exploit opportunities to improve the performance and sustainability of the company through the use of IT. |
| 5.3       | The board should delegate the responsibility for the implementation of an IT governance framework to management. | • 5.3.1. Management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework.  
• 5.3.2. The board may appoint an IT steering committee or similar function to assist with its governance of IT.  
• 5.3.3. The chief executive officer (CEO) should appoint a CIO responsible for the management of IT.  
• 5.3.4. The CIO should be a suitably qualified and experienced person who should have access and interact regularly on strategic IT matters with the board and/or appropriate board committee and executive management. |
| 5.4       | The board should monitor and evaluate significant IT investments and expenditure. | • 5.4.1. The board should oversee the value delivery of IT and monitor the return on investment from significant IT projects.  
• 5.4.2. The board should ensure that intellectual property contained in information systems is protected.  
• 5.4.3. The board should obtain independent assurance on the IT governance and controls supporting outsourced IT services. |
| 5.5       | IT should form an integral part of the entity’s risk management process. | • 5.5.1. Management should regularly demonstrate to the board that the company has adequate business resilience arrangements in place for disaster recovery.  
• 5.5.2. The board should ensure that the company complies with IT laws and that IT-related rules, codes and standards are considered. |
| 5.6       | The board should ensure that information assets are managed effectively. | • 5.6.1. The board should ensure that there are systems in place for the management of information, which should include information security, information management and information privacy.  
• 5.6.2. The board should ensure that all personal information is treated by the company as an important business asset and is identified.  
• 5.6.3. The board should ensure that an information security management system (ISMS) is developed and implemented.  
• 5.6.4. The board should approve the information security strategy and delegate and empower management to implement the strategy. |
Acknowledgment

This research is part of a co-created research project by KPMG Belgium, CEGEKA Belgium, Samsung Belgium, the Antwerp Management School and the University of Antwerp (Belgium). The leadership role of the industry partners in supporting this research is focused on better understanding the crucial accountability of the BoD in governing digital assets and providing solutions and tools for these board members to assume their accountability.

Endnotes

13 Environmental Corporate Governance Institute, “Index of Codes,” www.ecgi.org/codes/all_codes.php
15 Op cit, IT Governance Institute
16 Op cit, Joshi
18 Op cit, OECD
19 The next version of the Corporate Governance Code, King IV, will be released in 2017.

---

**Pinpoint your next job opportunity with ISACA’s CareerLaser**

ISACA’s CareerLaser newsletter offers monthly updates on the latest jobs, top-of-mind industry news, events and employment trends to help you navigate a successful career the information systems industry. Let CareerLaser become your top resource for quality jobs matched specifically to your talents in audit, assurance, security, governance, risk management and more.

Subscribe today by visiting [www.isaca.org/careerlaser](http://www.isaca.org/careerlaser)

Visit the ISACA Career Centre at [www.isaca.org/careercentre](http://www.isaca.org/careercentre) to find additional career tools, including access to top job candidates.
A Guide to Auditing Attachment Fields in Access Databases

Attachments are popular in several accounting contexts. Many of the same file types that can be attached to emails can also be attached to the records in databases. For example, a user could store PDF files of professional certifications in attachment fields, thereby helping to maintain complete records of employee accreditations. Examples of database attachment files include:

- Microsoft Word documents such as contracts, job applications, work orders and tax returns
- Photographs such as pictures of clients, assets and professional events
- Spreadsheets such as budgets and forecast projections
- Audio files such as WAV files of phone conversations
- Video files such as recordings of interviews with clients and job applicants
- Specialized files such as PowerPoint files of presentations and PDF files of legal documents

Because of the popularity of attachment fields, an auditor may encounter client data that include attached files or may be asked how best to store such information in database records. Some examples include contracts attached to customer or supplier records, employment records, various types of inspection reports and patient records. Clients may not give much thought to attachment fields, including why they should name or store them systematically. However, if attachment files require further inspection, auditors need to know how to create attachment fields in databases, how to advise clients why some naming or storage approaches are better than others, and how to query attachment fields effectively. These queries include the ability to automate tests for the:

- Existence of attachment files
- Absence of attachment files
- Ability to find specific types of attachments using various query tools

Microsoft Access is one of several databases that support attachment fields. Other popular systems include Oracle, Informix and most alternate Microsoft products, such as Microsoft SQL Server. Many database systems also allow users to download smaller data sets into Access (sometimes using third-party tools), which is a convenient

Joshua J. Filzen, Ph.D., CPA
Is assistant professor of accounting in the College of Business and Economics at Boise State University (Idaho, USA).

Mark G. Simkin, Ph.D.
Is professor of information systems in the College of Business at the University of Nevada (USA). He is the author or coauthor of more than 100 journal articles. His new book, Core Concepts of Accounting Information Systems, published by John Wiley and Sons, will be available in November of 2017.
The examples illustrate the tasks using Access 2016, but most of the discussions and figures also apply to Access 2013.

Creating and Viewing Attachments

Creating and viewing attachments in databases like Access is relatively straightforward. The discussions that follow briefly review these tasks for those unfamiliar with them.

Creating Attachment Fields

If a business owner wants to store electronic information about job applicants—for example, Word or PDF documents—one way to do this is to store them as attachments to each applicant’s record in an applicant database table. Figure 1 illustrates the design for this table, which lists some exemplary data fields and their data types. To create an attachment field:

1. Add a field for attachments to the main record list of fields.
2. Name the field (it does not have to be called “ApplicantAttachments” as shown in figure 1).
3. Select the “attachment” data type for the new attachments field from the drop-down list, as shown in figure 1.
4. To attach specific files to the attachments field, switch to the datasheet view (shown in figure 2) and double-click on the attachment field of a particular applicant’s record. This launches the Attachments dialog box (see the open dialog box in figure 2).

Note: Access replaces the field name (“ApplicantAttachments”) of an attachment data-type field with a paper clip symbol. To display the desired field name instead of the paper clip symbol, specify the desired field name (e.g., “Applicant Letters”) in the “Caption” setting of the Field Properties for this field.

Figure 2 illustrates that the content of attachment data-type fields (for example, in the first record) also contains the paper clip symbol. A “(0)” in the applicant-record Attachments field indicates that there are no attachments.

---

**Figure 1**—Defining an Attachment Data Field in Access

![Figure 1](source)

**Figure 2**—How to Add a File to an Attachment Field

![Figure 2](source)
5. To add attachments, click on the Add button in the Attachments dialog box. The Choose File dialog box (not shown) will be displayed.

6. In the Choose File dialog box, select the particular file to attach to the record and then click OK in the Attachments dialog box. The system returns to the data sheet view of records (figure 2). The paper clip (attachments) field for the applicant record contains (1), indicating that the attachments field now contains one attachment.

Attaching Multiple Files to a Record

Normally, each field of a database record can only contain one piece of information. The exception is the attachment data-type field of a record, which can contain multiple files.

To add another attachment to an attachment data-type field, repeat steps 5 and 6 in the previous section. Figure 3 illustrates the example applicant record with a picture file attachment and a résumé file attachment.

The ability to store multiple attachments in the same data field can be a disadvantage if the field contains many files. For example, if an Access table of car accidents contains picture files of accidents and written report files about them, then a single attachment data-type field may not be the best way to store them. In these instances, auditors can advise clients to create two attachment data-type fields per record—one to store pictures and a second field to store written reports. This approach can also improve the auditability of the database records.

Viewing Attachment Fields

An auditor can inspect the contents of attachment fields in two ways—in the datasheet view and in a database form.

Datasheet View

To view attachments in the datasheet view:

1. Go to the datasheet view (shown in figure 4), and double-click on the attachment field of an applicant’s record. This launches the Attachments dialog box (see the open dialog box in figure 4).

2. In the Attachments dialog box, either click the attachment name once to select it and then click the Open button on the right, or double-click the filename itself.

An attachment opens in its parent software, which Access launches when a user selects the attachment for viewing. For example, if the attached file is an Excel spreadsheet, then Access launches the Excel parent software. Opening attachments allows auditors to view

Figure 3—An Attachment Data Field With Two Attachments

Source: Microsoft Corporation. Reprinted with permission.

Figure 4—Viewing an Attachment Field in Datasheet View

Source: Microsoft Corporation. Reprinted with permission.

A paper clip symbol replaces the field name.

The number in parentheses is the number of attachments for this record.
filenames of other file types that are stored in the attachment field—a convenient way to view several attachment photographs quickly and speed up the audit process.

3. To open and view an attachment that is not a photograph (e.g., a Word document, PDF file, audio file or video file) and for which only a filename displays, double-click the filename in the attachment area of the form. Access will launch the appropriate parent software and open the file for viewing.

Attachment Field Rules

Figure 6 lists some important Access guidelines that auditors should know.

<table>
<thead>
<tr>
<th>Figure 6—Rules Governing the Creation and Use of Attachment Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The size of an attached file must be no larger than 256 Mb.</td>
</tr>
<tr>
<td>2. There is a maximum of 500 files per attachment field, but a record design can contain several attachment fields.</td>
</tr>
<tr>
<td>3. The attachments stored in a database are static and will not automatically update if new underlying data (e.g., a new applicant photograph) become available.</td>
</tr>
<tr>
<td>4. The maximum size limit for an Access database is 2 GB, which limits the total size or number of attachments that are stored in the database.</td>
</tr>
<tr>
<td>5. The contents of an attached file, e.g., the name of a company contained in a Word document attachment, are not searchable. Therefore, queries are constrained to the attachment field itself.</td>
</tr>
<tr>
<td>6. It is only possible to edit an attachment if the local computer has the necessary software, e.g., Microsoft Word if the attachment is a Word file. Edited files must be removed, modified and then reattached.</td>
</tr>
<tr>
<td>7. Users can only add or delete attached files through the Attachments dialog box.</td>
</tr>
<tr>
<td>8. If needed, Access compresses files that are uncompressed in attachments before storing them.</td>
</tr>
<tr>
<td>9. Generally, users can attach files from any location on their disk drives or networks.</td>
</tr>
<tr>
<td>10. Users can work with attachments programmatically, using Visual Basic for Applications (VBA) and the new Attachment object. This object supports a number of properties, methods and events.</td>
</tr>
</tbody>
</table>


Database Form View

A database form is a convenient way to view photograph attachments. To view attachments in a database form:

1. Create a database form for a database record (figure 5). When a form becomes active, Access displays the first photograph (or the filename of another file type, if photographs are not the only file type attached) of the attachment field in the record.

2. To quickly review additional files (photographs and other file types) in an attachment field, click the displayed photograph or filename in the attachment. A navigation bar displays above the field, as shown in figure 5.

Click the navigation bar arrows to scroll through and view additional photographs and the filenames of other file types that are stored in the attachment field—a convenient way to view several attachment photographs quickly and speed up the audit process.

In the dialog box of figure 4, be careful not to click the Remove button. Clicking the Remove button permanently deletes the selected file as an attachment, and the action cannot be undone. If an attachment is accidentally removed, it must be added as an attachment to the record again, using the instructions in the “Creating Attachment Fields” section, beginning with step 4.

Database Form View

A database form is a convenient way to view photograph attachments. To view attachments in a database form:

1. Create a database form for a database record (figure 5). When a form becomes active, Access displays the first photograph (or the filename of another file type, if photographs are not the only file type attached) of the attachment field in the record.

2. To quickly review additional files (photographs and other file types) in an attachment field, click the displayed photograph or filename in the attachment. A navigation bar displays above the field, as shown in figure 5.

Click the navigation bar arrows to scroll through and view additional photographs and the filenames of other file types that are stored in the attachment field—a convenient way to view several attachment photographs quickly and speed up the audit process.

3. To open and view an attachment that is not a photograph (e.g., a Word document, PDF file, audio file or video file) and for which only a filename displays, double-click the filename in the attachment area of the form. Access will launch the appropriate parent software and open the file for viewing.

Attachment Field Rules

Figure 6 lists some important Access guidelines that auditors should know.

<table>
<thead>
<tr>
<th>Figure 6—Rules Governing the Creation and Use of Attachment Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The size of an attached file must be no larger than 256 Mb.</td>
</tr>
<tr>
<td>2. There is a maximum of 500 files per attachment field, but a record design can contain several attachment fields.</td>
</tr>
<tr>
<td>3. The attachments stored in a database are static and will not automatically update if new underlying data (e.g., a new applicant photograph) become available.</td>
</tr>
<tr>
<td>4. The maximum size limit for an Access database is 2 GB, which limits the total size or number of attachments that are stored in the database.</td>
</tr>
<tr>
<td>5. The contents of an attached file, e.g., the name of a company contained in a Word document attachment, are not searchable. Therefore, queries are constrained to the attachment field itself.</td>
</tr>
<tr>
<td>6. It is only possible to edit an attachment if the local computer has the necessary software, e.g., Microsoft Word if the attachment is a Word file. Edited files must be removed, modified and then reattached.</td>
</tr>
<tr>
<td>7. Users can only add or delete attached files through the Attachments dialog box.</td>
</tr>
<tr>
<td>8. If needed, Access compresses files that are uncompressed in attachments before storing them.</td>
</tr>
<tr>
<td>9. Generally, users can attach files from any location on their disk drives or networks.</td>
</tr>
<tr>
<td>10. Users can work with attachments programmatically, using Visual Basic for Applications (VBA) and the new Attachment object. This object supports a number of properties, methods and events.</td>
</tr>
</tbody>
</table>

Creating Audit Queries of Attachment Fields

One of the advantages of using databases such as Access to store various types of data is the ability to create queries to find information quickly—a way of automating the audit process. This advantage also applies to attachment fields. For example, it could be used to identify all employees who do not have a current picture on file. If all of the picture files were organized in system file folders, the search might require a lengthy manual inspection, even though the storage medium is electronic. Alternatively, if the pictures were stored in the attachment fields of an Access database, a simple query can immediately identify all records that are missing photographs.

This section presents different ways that auditors can examine attachment fields in the context of a database table of job applicants. The methods discussed in this section are valuable in a variety of additional auditing contexts, such as examining lending documents, supplier contracts or other important business records that are stored as record attachments.

**Exact-match Queries**

Queries enable database users to identify the records of a database table that satisfy specific search criteria. One of the easiest ways to search for specific attachment files is by filename—for example, to verify the presence of a particular attachment document for a specific record. In Access parlance, this is an example of an exact-match query.

Access can search all record attachment files in a table of records and display only the record(s) containing the desired file(s). For example, to verify the presence of a photograph file named JoshPicture.jpg, create a query to search for this filename directly. Enter the full filename, including the file extension (.jpg) in the Criteria cell for the Attachments field (figure 7). The query finds the record containing the photograph file, even if the record contains several files in addition to the queried file.

**Figure 7** shows quotation marks around the filename. Access adds these marks automatically to signify that this is an exact-match query. Thus, it is not necessary to type them separately.

**Parameter Queries**

To view numerous pictures with known filenames, it may be helpful to use a parameter query to search for and display records containing photograph files, or view them in a database form (see the “Database Form View” section).

To create a parameter query (such as the one shown in figure 8):

1. Create the criterion “[What is the file name?]”. Be sure to include square brackets around the term. At run time, Access displays the Enter Parameter Value dialog box for the “What is the file name?” criterion.

2. Enter the full filename, with its file extension, in the Enter Parameter Value dialog box, and click

**Figure 7—An Access Query to Select a Specific File From an Attachment Field**

Source: Microsoft Corporation. Reprinted with permission.
“OK.” Access will display the record containing the photograph file.

3. To search for and display another photograph attachment, rerun the parameter query in figure 8 with the different filename.

The advantage of using parameter queries is that the auditor does not have to create new queries to find every desired file attachment. Instead, the auditor can rerun the same parameter query as many times as needed, thus speeding up the audit process.

**Wildcard Searches**

If the full name of a desired attachment file is unknown, a wildcard search can be used to create queries based on partial information. For example, suppose several audio filenames begin with the term “PhoneInterview,” such as PhoneInterviewFilzen.wav and PhoneInterviewSimkin.mp4, in a job-applicant table. To find all attachments that begin with PhoneInterview, add an asterisk (wildcard) after the known part of the filename (e.g., PhoneInterview*) in the Attachment field Criteria cell portion of the query. Access will find all records whose attachment files begin with “PhoneInterview,” including PhoneInterviewSimkin.mp4 and PhoneInterviewFilzen.wav.

Multiple wildcards can be used in the same query. For example, suppose an attachment field contains the files “2016PhoneInterviewSimkin.mp4” and “2017PhoneInterview.wav.” An Access query using the criteria “PhoneInterview*” (with wildcards at both the beginning and end of the search criteria) finds the records for both of the files, plus all records in the table that contain this criteria—not just the phone interview files for a desired client. This problem can be overcome by including the client name as an additional search element in a separate criteria field of the query (see the “Too Many Record Hits?” section).

Knowing how to use wildcards enables auditors to find, for example, all picture files ending in .jpg (using *.jpg as the search criteria) or .gif (using *.gif as the search criteria). These are searches that look for file types instead of filenames. In each case, Access automatically embeds the LIKE operator with the wildcard criteria, as illustrated in figure 9 for the first example. When the query in figure 9 runs, the displayed result shows all records with attachment filenames that end in .jpg.

The OR operator can be used in wildcard queries to find filenames satisfying two (or more) alternate endings (or beginnings). For example, to find .jpg or .gif files, use the compound criteria shown in figure 10. This query identifies all files with filenames ending in “.jpg” or “.gif.” An alternate way to express an OR condition is to enter each file type query on separate lines under the Attachments field, which might be easier if there are more than two or three conditions.

---

**Figure 8—Example Parameter Query and Enter Parameter Value Dialog Box**

Source: Microsoft Corporation. Reprinted with permission.

**Figure 9—Access Wildcard Query to Find all Attachment Files Ending in .jpg**

Source: Microsoft Corporation. Reprinted with permission.

**Figure 10—Wildcard Search Using the OR Operator**

Source: Microsoft Corporation. Reprinted with permission.
The availability of wildcard searches provides motivation for naming files systematically to facilitate the ability to audit them later. An example is using the naming convention PhoneInterview Name for the name of all files that are recordings of phone interviews.

**Too Many Record Hits?**
The query examples in this article are generic and may result in thousands of returned records in large database tables. One way to narrow the search is to use additional fields in a record to specify additional search requirements. For example, to see a list of all photograph files for the client Thomas Trenton, simply include the first and last name in the search criteria. Additional field criteria (figure 11) narrow the list considerably, because all search criteria listed on the same criteria line in an Access query specify an AND condition. The search criteria in figure 11 instructs Access to display all records containing .jpg or .gif files only for Thomas Trenton.

**Testing for the Absence or Presence of Attachments**
An auditor may want to confirm that the Attachment field in each record is not empty. This task can be automated in Access. For example, to confirm that all job-application records include résumés, use “Is Null” in the query to identify missing résumé attachments. Be sure to include a space in this term. Figure 12 illustrates the appropriate query.

When the auditor runs this query, the results are a datasheet that displays all job applicant records that are missing résumés in the Résumé Attachment field. This approach does not work for attachment fields that store résumés and other files, e.g., photographs, in the same attachment field. The query in figure 12 only lists records that contain nothing in their attachment fields. Finally, it is also a simple matter to search for nonblank data fields using the NOT operator. In effect, the expression “Not Is Null” creates a query that displays all records that contain something in the data field of interest. Figure 13 illustrates the query for job applicants with résumés. The results are a datasheet listing all records that have files in their Résumé attachment field. For a certification application that stores PDF files of test results, for example, using the “Not Is Null” expression in a query allows an auditor to identify those employees who have taken a required test.

---

**Figure 11**—Access Query to List all JPEG or GIF Files for Thomas Trenton

<table>
<thead>
<tr>
<th>Field</th>
<th>Table</th>
<th>Sort</th>
<th>Show</th>
<th>Criteria: or</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastName</td>
<td>tblClients</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FirstName</td>
<td>tblClients</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachments</td>
<td>tblClients</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;Thomas&quot;</td>
<td></td>
<td></td>
<td></td>
<td>&quot;<em>.jpg Or Like &quot;</em>.gif&quot;</td>
</tr>
</tbody>
</table>

*Source: Microsoft Corporation. Reprinted with permission.*

**Figure 12**—Query to Identify Records With Blank Résumé Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Table</th>
<th>Sort</th>
<th>Show</th>
<th>Criteria: or</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>tblClients2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LastName</td>
<td>tblClients2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>tblClients2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resume</td>
<td>tblClients2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Is Null</td>
</tr>
</tbody>
</table>

*Source: Microsoft Corporation. Reprinted with permission.*

**Figure 13**—A Query to Identify Records Containing Résumés

<table>
<thead>
<tr>
<th>Field</th>
<th>Table</th>
<th>Sort</th>
<th>Show</th>
<th>Criteria: or</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>tblClients2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LastName</td>
<td>tblClients2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>tblClients2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resume</td>
<td>tblClients2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not Is Null</td>
</tr>
</tbody>
</table>

*Source: Microsoft Corporation. Reprinted with permission.*
Conclusion

The advantages of using attachment fields in databases are considerable, enabling users to store multiple photographs, Word documents, spreadsheets, PowerPoint presentations and similar files in electronic formats; consolidate information from several locations; and perhaps come closer to the ideal of a paperless office. Because of these advantages, auditors may find themselves in a situation where they need to retrieve or verify information stored in attachment fields. Some key items for auditors to keep in mind regarding the use of attachments in Access include:

- Modern database software enables users to attach, and auditors to query, attachment files conveniently—for example, to create queries by filename, by file format, by client name or by some combination of these criteria.

- Encouraging clients to name files consistently, using embedded generic terms such as interview or photo, helps users to organize attachments logically and helps auditors to identify them more easily, as needs require.

- Auditors can test for the presence or absence of attachment files and identify types of file attachments using wildcard file extensions. However, Access does not allow auditors to test the contents of attached files.

- The information that is typically stored in a database is sensitive and attachments typically contain information that increases this sensitivity. For this reason, auditors should encourage clients to protect database information with passwords and create backup copies of their databases.
Key Ingredients to Information Privacy Planning

The metrics associated with privacy data breaches are astounding. In 2016, 554,454,942 records were breached from 974 reported incidents. To break down the type of data affected, 48 percent of data breach incidents were for personally identifiable information (PII), 27 percent were for credit and debit card data, and 11 percent were for physical health information (PHI).

The root causes of privacy incidents include the outsourcing of data, malicious insiders, system glitches, cyberattacks, and the failure to shred or dispose of privacy data properly. The human element of data breaches is the result of social engineering, financial pretexting (the practice of obtaining personal information under false pretenses), digital extortion, insider threat and partner misuse. Conduit devices used include Universal Serial Bus (USB) infection, rogue network connections, manipulation of account balances and backdoor access accounts. Configuration exploitation and malicious software are also causes of data compromises.

This article will review many aspects of privacy and is intended as a primer for information privacy. Topics to be reviewed are categories of privacy, privacy officer (PO) concerns, governance strategy, privacy controls and the privacy plan.

Categories of Privacy

ISACA® has identified seven categories of privacy that every enterprise must address, as shown in figure 1.

Privacy Information Concerns

To address the personal and organizational concerns of data privacy, the position of PO was created. Figure 2 shows data concerns, areas of risk and questions the PO must ask.

All of these concerns help to identify the scope and complexity of the work. Data governance methods and techniques that need to be employed include data identification, protective measures, intrusion detection monitoring and reporting, responding to privacy events and incidents, and recovery of the organization to normalcy (when possible).

Governance Activities

Governance of privacy-related information requires that a custom strategy be developed for any organization. Governance activities should include:

- Identifying the stakeholders and internal partnerships.
- Developing vision, mission and value statements with goals and objectives. This information would be a reference and resource for a privacy charter that can be used throughout the course of the privacy policy development effort.
- Establishing connections within the organization to ensure cooperation and efficiency.
- Writing a privacy policy (described in a following section) to address warning banners; system compromise alerts; key persons to contact; and response, containment, and recovery processes and procedures.
- Developing a data governance strategy that includes data collection, authorized use, access controls, information security and destruction of the data/information. The key functional aspects are assessment, protection, sustaining privacy operations and responding to compromises.
- Establishing a privacy budget that includes outreach activities and a contingency reserve for recovery and emergency expenditures. The expenditures would include forensic investigations, victim notification, call center support, outside counsel (e.g., litigation costs), security enhancements, lost revenue and stock value, insurance, remediation actions, punitive costs (e.g., civil penalties and fines), customer retention, card replacement, victim damages, and opportunity costs.

The metrics associated with privacy data breaches are astounding. In 2016, 554,454,942 records were breached from 974 reported incidents. To break down the type of data affected, 48 percent of data breach incidents were for personally identifiable information (PII), 27 percent were for credit and debit card data, and 11 percent were for physical health information (PHI).

Governance of privacy-related information requires that a custom strategy be developed for any organization. Governance activities should include:

- Identifying the stakeholders and internal partnerships.
- Developing vision, mission and value statements with goals and objectives. This information would be a reference and resource for a privacy charter that can be used throughout the course of the privacy policy development effort.
- Establishing connections within the organization to ensure cooperation and efficiency.
- Writing a privacy policy (described in a following section) to address warning banners; system compromise alerts; key persons to contact; and response, containment, and recovery processes and procedures.
- Developing a data governance strategy that includes data collection, authorized use, access controls, information security and destruction of the data/information. The key functional aspects are assessment, protection, sustaining privacy operations and responding to compromises.
- Establishing a privacy budget that includes outreach activities and a contingency reserve for recovery and emergency expenditures. The expenditures would include forensic investigations, victim notification, call center support, outside counsel (e.g., litigation costs), security enhancements, lost revenue and stock value, insurance, remediation actions, punitive costs (e.g., civil penalties and fines), customer retention, card replacement, victim damages, and opportunity costs.
<table>
<thead>
<tr>
<th>Category</th>
<th>Area of Concern</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data and image (Information)</td>
<td>Rules that govern the collection and handling of personal information</td>
<td>• Financial information&lt;br&gt; • Medical information&lt;br&gt; • Government records&lt;br&gt; • Records of personal activity</td>
</tr>
<tr>
<td>Person/bodily</td>
<td>Person’s physical being and invasion thereof</td>
<td>• Genetic testing&lt;br&gt; • Drug testing&lt;br&gt; • Body cavity searches&lt;br&gt; • Birth control&lt;br&gt; • Abortion&lt;br&gt; • Adoption</td>
</tr>
<tr>
<td>Communications</td>
<td>Protection of the means of communication</td>
<td>• Postal mail&lt;br&gt; • Telephone conversations&lt;br&gt; • Email&lt;br&gt; • Hidden microphones&lt;br&gt; • Other forms of communicative behavior and apparatus&lt;br&gt; • Not informing citizens when surveillance occurs</td>
</tr>
<tr>
<td>Thoughts and feelings</td>
<td>Protection of individuals to ensure that their thoughts and feelings are not shared inappropriately with others, or they are not forced to share and have negative impacts against them in some way</td>
<td>• Being forced to provide social media passwords when applying for a job&lt;br&gt; • Being forced to reveal religious beliefs or political views when applying for a job</td>
</tr>
<tr>
<td>Association</td>
<td>Addresses the right people have to associate with anybody they wish to, without unauthorized monitoring or marginalization, and addresses the types of groups that individuals belong to, for which they have no control, e.g., ethnicity or ancestry</td>
<td>• DNA testing that demonstrates ethnicity or ancestry&lt;br&gt; • Denying membership of any kind after DNA testing revealed predisposition to an “undesirable” condition&lt;br&gt; • Employers using DNA testing to make termination decisions&lt;br&gt; • Any type of segregation based on religion, behavior, assembly or membership</td>
</tr>
<tr>
<td>Location and space (Territorial)</td>
<td>Concerned with placing limits on the ability to intrude into an individual’s location, space and general environment. The environment is not limited to the home; it also includes the workplace and public spaces. Invasion into an individual’s territorial privacy typically takes the form of monitoring, such as video surveillance, the use of drones, identification checks and use of similar technology and procedures.</td>
<td>• Home&lt;br&gt; • Workplace&lt;br&gt; • Public space&lt;br&gt; • Video surveillance&lt;br&gt; • ID checks&lt;br&gt; • Other technology, e.g., flying a drone over an individual’s property to take photos&lt;br&gt; • Recording individuals behind their property fence</td>
</tr>
<tr>
<td>Behavior and action</td>
<td>This is an extension of a person’s privacy. It is focused on thoughts and emotions before they are expressed to somebody, activities in public and private, and targeted monitoring.</td>
<td>• Sexual preferences&lt;br&gt; • Political views&lt;br&gt; • Religious beliefs and activities&lt;br&gt; • Use of traffic signal cameras to catch those who commit traffic violations&lt;br&gt; • Use of police body cameras</td>
</tr>
</tbody>
</table>

Source: L. Wlosinski. Reprinted with permission.
<table>
<thead>
<tr>
<th>Concern</th>
<th>Area of Risk</th>
<th>Description/Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laws and regulatory landscape</td>
<td>Compliance, penalties, fines, public embarrassment, and loss of business and revenue</td>
<td>• Each country has its own version of what privacy means and has laws for the types of privacy data. The PO should be familiar with the laws, directives, standards, guidelines and policies that can be developed by the government, professional associations and the organization itself.</td>
</tr>
</tbody>
</table>
| Type of data                                 | Exposure of personal information; exposure of business sensitive, confidential or classified information trade secrets; inability to control or manage data securely | There are many questions associated with data type:  
• Are the data considered PII?  
• Are the personal data medical in nature (e.g., person’s current health, medical history, DNA information)?  
• Are the data personal financial data, such as salary, loans, amount of debt or credit history?  
• Are the data about records of personal activity or history (e.g., level of clearance, citizenship, arrest record, association membership, web activity)?  
• What is the information medium (e.g., text, audio, video, email, screen captures, photo or paper format)? |
| Amount of data                               | Not knowing where the data exist and, consequently, not being able to control the data | • How many systems have privacy data?  
• How many records are in the system?  
• How many devices store and process the data?  
• How many data are accumulated daily, weekly and monthly?  
• How long does the government and/or the business require the data to be stored and protected? |
| Location of data                             | Unauthorized access, use or disclosure of data; unable to investigate or litigate if offshore offender; unable to protect data | • How many locations are affected (e.g., primary facility, mirrored facility, off-site backup files, cloud service providers, contractor-managed facilities)?  
• Are the data on social media or on a website (by accident or by malicious intent)?  
• Do the data reside in retired systems and data stores? |
| Source of data                               | Not acquiring accurate information; obtaining the data illegally | • How is the information gathered?  
• Do the data exist in an internal system or in hard copy?  
• Do the data come from an external business partner?  
• Are the data from a major application or a general support system (GSS) in the organization?  
• Were the data obtained by internal and/or external surveillance devices (e.g., cameras, drones)?  
• Are cookies used by company web applications? |

Enjoying this article?  
• Read A Privacy Principles and Program Management Guide. www.isaca.org/privacy-principles  
• Learn more about, discuss and collaborate on information security policies and procedures in the Knowledge Center. www.isaca.org/information-security-policies-and-procedures
Performing impact assessments/audits. A privacy impact assessment (PIA) questionnaire should be used to inform the PO of possible concerns and potential problems when a computer system is developed or changed. The PIA should identify the types of data, the scope of people affected, the type of information, any new information obtained and the other concerns described previously.

<table>
<thead>
<tr>
<th>Concern</th>
<th>Area of Risk</th>
<th>Description/Questions</th>
</tr>
</thead>
</table>
| Availability of data          | Production; not having the data when needed; other party involvement | • Are the data available publicly via the Internet, internally on the intranet or remotely via a virtual private network (VPN) connection?  
  • Will the data be available via a new system?  
  • Are production data of a private nature and used by the developers when testing the system?  
  • Are the data shared with other organizations/partners?  
  • Has the organization employed data minimization techniques for privacy-related data?  
  • Who has access to the data?  
  • Are the data accessible by mobile devices (e.g., smartphones, tablets, laptops)?  
  • How will the data be shared/exchanged? |
| Protective measures           | Poor or inadequate device configuration protection | • Does the organization employ technical protective measures such as account authentication (e.g., account with a password), user access cards, multifactor authentication, data encryption in transit and at rest, network protective devices and software, software updates and patches?  
  • What data integrity controls are in place, and are they effective?  
  • Are the system access control lists checked on a regular basis for leftover accounts (that could be used as backdoors into the system)?  
  • Are physical access controls in place? |

Source: L. Wlosinski. Reprinted with permission.
Privacy audits can measure effectiveness, demonstrate compliance, increase awareness, reveal gaps, and provide a basis for remediation and improvement plans. PIAs can be at all levels, e.g., department, system and process.

- Establishing a continuous monitoring program. Does the PO receive system monitoring and network access tracking information? Is the PO informed of the results of independent and/or internal systems assessments? Does the assessment cover all of the necessary privacy controls (which are mentioned in the following section)? Have all remedial actions been performed to limit the possibility of a privacy incident? Noncompliance reports should answer the questions what, where, when, why, who and how.

• Providing an information privacy awareness and training program. This could include developing awareness brochures and flyers for internal staff and contractors. All employees, business partners and contractors need to be trained on the privacy policy and procedures.

• Developing a public privacy website to explain the program and display whom to contact with questions. It could also include frequently asked questions.

• Ensure that the contingency and disaster recovery plans can recover the data.

Privacy Controls

There are four types of privacy controls: management, computer operations, business operations and technical. Implementing the controls is critical to a successful privacy program. If time permits, they should be implemented in the following order: identify areas of concern, implement protective measures, install detection mechanisms and employ response management techniques.

The four types of privacy controls are described as follows.6

1. Management controls

- **Identification**—Responsibilities include documenting legal authority, scrutinizing the new uses of PII, and having an inventory of PII programs and systems.

- **Protective measures**—Management must monitor laws for changes; appoint the PO; provide funding; update procedures and tools; explain the privacy program; assign roles and responsibilities; define privacy statements on contracts, acquisition documents and websites; issue privacy notices, policies and procedures; develop a strategic privacy plan; identify and explain why PII is collected; limit the collection and retention of PII; design systems to support privacy (e.g., data minimization); issue data integrity guidance; have privacy audits can measure effectiveness, demonstrate compliance, increase awareness, reveal gaps, and provide a basis for remediation and improvement plans. PIAs can be at all levels, e.g., department, system and process.

- Establishing a continuous monitoring program. Does the PO receive system monitoring and network access tracking information? Is the PO informed of the results of independent and/or internal systems assessments? Does the assessment cover all of the necessary privacy controls (which are mentioned in the following section)? Have all remedial actions been performed to limit the possibility of a privacy incident? Noncompliance reports should answer the questions what, where, when, why, who and how.

• Providing an information privacy awareness and training program. This could include developing awareness brochures and flyers for internal staff and contractors. All employees, business partners and contractors need to be trained on the privacy policy and procedures.

• Developing a public privacy website to explain the program and display whom to contact with questions. It could also include frequently asked questions.

• Ensure that the contingency and disaster recovery plans can recover the data.

Privacy Controls

There are four types of privacy controls: management, computer operations, business operations and technical. Implementing the controls is critical to a successful privacy program. If time permits, they should be implemented in the following order: identify areas of concern, implement protective measures, install detection mechanisms and employ response management techniques.

The four types of privacy controls are described as follows.6

1. Management controls

- **Identification**—Responsibilities include documenting legal authority, scrutinizing the new uses of PII, and having an inventory of PII programs and systems.

- **Protective measures**—Management must monitor laws for changes; appoint the PO; provide funding; update procedures and tools; explain the privacy program; assign roles and responsibilities; define privacy statements on contracts, acquisition documents and websites; issue privacy notices, policies and procedures; develop a strategic privacy plan; identify and explain why PII is collected; limit the collection and retention of PII; design systems to support privacy (e.g., data minimization); issue data integrity guidance; have

- Instituting metrics. Metrics should be specific/simple, manageable, actionable, relevant/results-oriented and timely (SMART). Examples of privacy metrics include number of privacy data systems, percentage of data lost, number of privacy incidents, number of systems affected, average time between incidents and average time to recover. Privacy events may not always be large or computer-oriented in nature, but might occur on a small scale, e.g., identity theft.

- Implementing a privacy incident response plan (PIRP). To quickly respond to data breaches, the PO must be informed of all breaches and have information about the data and systems compromised. The breach plan should include a questionnaire/form, roles and responsibilities, points of contact information (e.g., security, management, legal, public relations, governing organizations), and communication procedures.
A privacy plan must include information for management, data handling operations (e.g., the data center or service provider), business operations and technical controls.

2. Computer operations controls
   • Identification—Identify systems and files affected.
   • Protective measures—Responsibilities include implementing and maintaining data protection and spillage prevention systems; protect PII in testing, training and research; developing and maintaining a PIRP; and training and monitoring staff.
   • Detection—Operations needs to write incident and activity reports for management.
   • Response management—Responsibilities include training for and providing forensic support; issuing spillage and data breach alerts; and using approved methods to delete or destroy PII as prescribed by management.

3. Business operations controls
   • Identification—Identify what business operations are affected.
   • Protective measures—Measures include approving website content, explaining the consent and information usage program, and obtaining consent of the affected party when applicable.
   • Detection—This activity includes monitoring business practices for fraud, identity theft and data misuse.
   • Response management—This area covers data spillage-handling activities, tracking and retaining records of disclosure, notifying those affected, supplying information to requestors, correcting erroneous PII, explaining individual rights, managing complaints, and responding to privacy spillage incidents.

4. Technical controls
   • Identification—This activity includes reviewing and assessing security tools and determining if other tools need to be acquired and implemented.
   • Protective measures—Measures include account authentication (e.g., account with a password); providing user access cards; using multifactor authentication, automatic time-out and external/remote access controls; data encryption in transit and at rest, network protective devices and software; software updates and patches; data integrity controls; technical control testing; and sanitizing and destroying data in compliance with government regulations.
   • Detection—This category includes the use of data mining software and cyberdetection techniques. It could also include the use of surveillance software in the systems infrastructure and devices in the building, as well as system and application transaction audit controls.
Privacy Plan

A privacy plan must include information for management, data handling operations (e.g., the data center or service provider), business operations and technical controls. The plan content should include the following:

- **List of authorities**—This list identifies who is dictating the compliance and reporting requirements and could also include the source of guidance and standards.

- **Definitions**—The types of privacy data must be defined to support the information contained in the plan.

- **Scope and purpose**—The plan should state who is affected by the plan, a general description of the plan and why it was written.

- **Roles and responsibilities**—The roles of various enterprise areas, including the PO, the office of information security, legal department, human resources, public relations, marketing, business development, finance and customer care need to be listed in the privacy plan. It is important for each area to know what needs to be communicated and what needs to be done, in what order and in what time frame. This should be supplemented by training and periodic tabletop exercises.

- **Privacy controls**—The plan should describe the requirements of the four categories of controls (previously described) and how the controls are to be implemented.

- **Other considerations**—This part of the plan would address areas of the governance strategy not covered and could be oriented to the industry or area of personal concern (e.g., financial, medical). A list of acronyms may also be needed.

---

**Conclusion**

The PO must identify the data, understand the business use of the data, protect the data, detect when the data are in jeopardy or have been exposed, and know how and what to do about it. Joining privacy associations, subscribing to privacy-related journals, following best practices from privacy organizations and having a comprehensive privacy plan will help to protect the data and everyone involved.

---

**Endnotes**

5. International Association of Privacy Professionals (IAPP), Privacy Program Management: Tools for Managing Privacy Within Your Organization, USA, 2013
A key issue often cited by information systems (IS) executives in the last three decades is aligning IT with business, which assists in realizing value from IT investments. This article demonstrates how a multinational oil company deployed an automated implementation of the Information Technology Infrastructure Library (ITIL) integrated with COBIT® in an effort to achieve alignment between IT goals and business goals. The article, based on a longitudinal study conducted over a period of three-and-a-half years (2012 to 2017), presents the challenges, value realized and lessons learned in moving from the planning stage of implementing an IT service management (ITSM) strategy to the dynamic phase of managing and distilling business value from IT.

Research indicates that alignment of IT and with the business has been the top IT management concern for three consecutive years since 2013, and has remained within the top three since 2005.¹ “Alignment” has been defined as the degree of fit and integration between business strategy, IT strategy, business infrastructure and IT infrastructure.² Hence, IT is considered to be very important to the delivery of the overall business strategy and vision, where the contribution of IT to the business is widely recognized, with value creation of IT investments being one of the most important dimensions.³ Subsequently, getting value from IT investments has been a top priority for organizations. Moreover, one of the four major activities of chief information officers (CIOs) is IT services, which encompass managing the IT organization, its people and its external partners to ensure delivery of IT infrastructure, applications, projects and related services across the enterprise at the desired cost, risk and service levels.⁴

Profile of Case Study Company

The company is a 24-year-old government-owned multinational oil company, registered and headquartered in the United Arab Emirates (UAE). Its annual revenue was US $14.7 billion in 2015. As of 2014, it had 39 companies in its portfolio, with more than 250 remote locations and diversified operations. The company has more than 6,500 employees. It directly or indirectly owns 39...
companies which operate through four business segments:

- **Supply, trading and processing**—Condensate and gas processing and oil trading
- **Terminals**—Storage for various petroleum and chemical products
- **Marketing**—Marketing of aviation fuel, lubricants, chemicals and industrial products
- **Retail**—Retail fuel and nonfuel services at retail stations

**IT Department Profile**

The IT department at the company head office manages the IT services of the entire group of companies using its own resources and outsourcing several IT services (figure 1). The IT department consists of 89 full-time equivalent (FTE) employees in four departments covering policy and planning, IT service, infrastructure, and business solutions. As part of a continuous improvement program, the IT service department was restructured in May 2016 (figure 2).

The IT architecture, which consists of five mainframes, 165 physical servers, 200 virtual servers, 650 network devices and 2,200 desktops, presents a challenging environment for the company in its operations. Interviews were conducted with the following personnel:

- **Director of IT services**—For overall strategy
- **IT service manager**—For customer satisfaction and service catalog
- **IT infrastructure manager**—For availability management, change management, release management

---

**Figure 1—IT Organizational Structure**

experience in establishing processes and procedures in his previous organization. He was entrusted with the major responsibility of managing in-house IT with four clear priorities to realize value from IT:

1. Setting up a world-class shared services center
2. Implementing best practices in ITSM for high-quality service delivery
3. Developing an efficient cost-recovery model with a well-defined IT service catalog for recharge transparency
4. Bringing in process automation and innovation for faster time-to-market services and products

His first jobs were to invest judiciously in IT and evaluate the current application to add value. He decided to scrap the current help-desk application and invest in what was needed to achieve the organization’s vision of what an ideal IT service organization should be and how these challenges should be addressed.

Therefore, he continued augmenting the initial cost of operation with a long-term view. He gave the go-ahead to invest in IT in contrast to maintaining an attitude of containing cost and working with limited resources. His position was not to cut costs, but that the organization should benchmark itself with the

**IT Governance Process and Leadership**

The company started to plan for ITSM implementation in September 2009. During that time, it underwent major restructuring and brought in a new CIO to lead the ITSM implementation. To restructure the IT service management function, the company appointed a new director of IT to oversee the IT functions of the entire group of companies. The newly appointed director of IT had a lot of vision and

---

“**In its ITSM implementation journey, the company proved that IT/business strategic alignment can be facilitated through the organization’s appropriate management practices and strategic IT choices.**”

---

**Source:** M. Nicho, S. Khan and R. Mohan. Reprinted with permission.
industry leader. Therefore, there were industry class systems that were needed and implemented.

**ITIL Phases**

In its ITSM implementation journey (figure 3), the company proved that IT/business strategic alignment can be facilitated through the organization’s appropriate management practices and strategic IT choices. In line with the principle of starting with relevant and simple processes, in phase 1 the organization implemented a 24/7 call center with an interactive voice response (IVR) integrated to the help desk, incident management, problem management, change management, and the creation of foundation data for service management and service level management.

Based on the lessons learned from this phase, the second phase saw the introduction of outage management, setting up of the customer care systems with a toll-free number and establishment of incident handling in another division. These accumulated experiences enabled the organization to move to phase 3, which consisted of release management (initial phase: user acceptance test only), upgrade of outage management, creation of IT work order billing information, the automation of service operating procedure (SOP) and creation of a configuration management database (CMDB).

Phase 4 started with the implementation of release and quality management, which involved a full-fledged quality management system incorporating the entire software development life cycle (SDLC) as part of release management. The automated ITSM tool (product) upgrade that started in quarter 2 of 2016 was still ongoing as of March 2017. This task entails upgradation of the automated ITSM tool to enable IT service mobility for support personnel and end users.

**Alignment of Business and IT Goals With IT Service Processes**

Midway through the ITSM journey, one of the exercises was to align 17 business goals (based on the four quadrants of the balanced scorecard [BSC]) to 28 IT goals. This was aligned subsequently to key ITIL and governance processes, and then further mapped to ISO 20000 and COBIT® controls (figure 4) using a proprietary IT governance tool (based on COBIT© 4.1) developed by an external consultant.

Within the tool, an analysis of the business and IT goals and an overview of the impact of certain IT risk factors on the organization were used to assess and select the COBIT processes relevant to the organization. Once this was completed, the tool allowed for a maturity assessment to be performed on these processes. In 2013, the organization created

**Figure 3—Timeline of the Ongoing ITSM Journey as of March 2017**

a strategy map with value drivers (Figure 5) for guidance in measuring the four quadrants of the BSC.

For each of the 14 value drivers (F1 to LG4), the organization drafted value driver statements for the four quadrants.

**Financial**

IT will:

- Maintain the ratio of IT operational expenditure (OPEX) to the company’s OPEX. (F1)
- Adhere to the approved budget. (F1)
- Ensure IT cost recovery based on the approved budget. (F2)
- Achieve benefits on identified projects and initiatives by effective resource utilization. (F2)

**Customers**

IT will:

- Deliver quality and reliable services that meet or exceed agreed service-level targets. (C1)

---

**Figure 5—Alignment of Business and IT Goals to IT Service Processes**

Providing ENOC with innovative and cost-effective IT solutions, and services optimally combined with world-class standards of services, quality and operational effectiveness

---

**Operational Excellence**

- C1. Deliver quality and reliable IT services
- IP1. Streamline key operational processes

**Customer Management**

- C2. Meet or exceed customer’s expectation
- IP2. Improve customer partnership

**Stakeholders**

- C3. Achieves “reliable business partner” image
- IP3. Develop and provide strategic and innovative business solutions

**Strategic Support**

- C4. Support customers’ key strategic objectives
- LG1. Create positive work environment
- LG2. Develop key competencies
- LG3. Leverage technology and knowledge assets

---

**Value Creation**

- F1. Optimize resource utilization

---

**IT Risk Assessed to Align Select IT Goals With IT Controls and Processes**

17 Business Goals (3 financial, 6 customer, 6 internal and 2 learning of the BSC)

28 IT Goals

Mapped to ISO 20000

---

Conclusion

Transitioning from a cost-centered IT service approach to creating value out of IT investments requires strong leadership, restructuring of IT and organizational hierarchy, alignment of IT goals with business goals, and deploying the balanced scorecard to assess their maturity level. These three activities enable the enterprise to clearly envision the IT service-specific challenges that are ahead and learn from the incremental implementation of ITIL processes for continuous improvement of IT services.

Endnotes

3. ISACA® and the IT Governance Institute, Global Status Report on the Governance of Enterprise IT (GEIT), USA, 2011.
Mobile has arisen as one of the most flexible—and most prevalent—business tools available. From email to calendaring to business applications, employees are, quite literally, doing business from any device, any time of the day or night, from anywhere and everywhere on the planet. Mobile functionality has evolved from a convenience to a necessity, from a luxury to a necessary and critical component of the business environment.

As mobile has increased its business utility, it has also become one of the more challenging areas to safeguard. Not only is bring your own device (BYOD) becoming the norm in many enterprises, bringing with it an array of disparate devices into the workplace, but the increase in sophistication of both mobile devices and the applications (apps) that reside on those devices means a wider array of security and assurance challenges than has ever before been the case. Granted, it is true that both organizations and practitioners are becoming more sophisticated in their approaches to mobile and, thereby, are becoming better able to anticipate and respond to challenges in the mobile space. However, it is still very much an area of focus for organizations as it continues to represent one of the leading attack vectors and a large chunk of the overall enterprise attack surface.

Because of this, savvy practitioners are always on the hunt for tools and techniques they can apply and adapt to help them ensure that devices are protected appropriately. Fortunately, there are quite a few good tools and resources out there that are available for relatively little (or no) cost.

Note that the tools described in this article are not the only tools out there—nor is this list intended to be an exhaustive one. This article’s focus is specifically on tools that are freely available—open source, community-supported editions of commercial tools, free resources, etc. These tools, indexed by category, might help solve specific security and assurance challenges relative to the mobile environment. Some of them pertain to testing scenarios on the mobile devices themselves, others relate to ensuring known-good configuration, and still others relate to leveraging older mobile devices (always easy to come by) to accomplish other security and assurance tasks.

Endnotes

1. Mobile Application Testing Tools

For those organizations that have the skill set internally to perform hands-on testing, there are a number of tools that can assist in the testing of mobile devices themselves or the business applications they commonly run. Insofar as testing of applications goes, web proxying tools such as Burp Suite (https://portswigger.net/burp/) and Open Web Application Security Project's (OWASP) ZAP (https://www.owasp.org/index.php/OWASP_Zed_AttackProxy_Project) are excellent choices. These tools allow users to “snoop” on traffic between the mobile device (or, really, any device) and web applications with which they interact. A web testing proxy such as this intercepts messages to the mobile device and the application and allows the manipulation of various parameters (e.g., HTTP headers, response parameters) in between the mobile device and the web application. Note that these tools are useful outside of the mobile device world as well; they can be used to test any web application regardless of the platform on which it is employed. However, because mobile device use is tied so closely to the applications they run, they are addressed here.

2. Mobile Device Testing Tools

In terms of specific testing of the mobile devices themselves—including malicious applications and testing of user behavior such as responding to phishing or Smishing (phishing via short message service [SMS])—there are some fantastic options as well. The first one is the community version of Shevirah’s Dagah tool (https://www.shevirah.com/dagah/). Those in the penetration testing space may recall the Smartphone Pentest Framework (www.bulbsecurity.com/products/smartphone-pentest-framework/), developed by Georgia Weidman in response to the Defense Advanced Research Projects Agency’s (DARPA) now-defunct Fast Track grant. The community edition does have some limitations (in terms of number of targets per campaign), but it does provide the tester with the ability to target mobile devices and customize attack scenarios and delivery of those attacks to a mobile device. There are even video instructions that explain common usage scenarios.

3. Mobile Forensics Tools

Of course, situations arise whereby one may need to investigate a device to determine if the device has been attacked—or to otherwise evaluate a potential incident impacting a mobile device. If one is investigating a specific device from an investigation standpoint, a fantastic resource to have in any arsenal is the Santoku Linux distribution (https://santoku-linux.com/). Santoku is an entire Linux distribution dedicated specifically to mobile device forensic examination. Other testing and incident response platforms do contain mobile tools; for example, both Kali (https://www.kali.org/) and CAINE (www.caine-live.net/) contain mobile analysis tools. However, Santoku has the advantage of being entirely designed specifically from a mobile analysis perspective.

4. OS Management Tools

From a device management standpoint, there are a few options as well. Not only are there tools that are built into the ecosystems of both Android and iOS, for example, the Apple Configurator (https://support.apple.com/apple-configurator) and the Android Device Manager (https://www.google.com/android/devicemanager), but there are also tools that provide privacy tools (e.g., The Guardian Project [https://guardianproject.info/] and hardened OS configurations (e.g., CopperheadOS [https://copperhead.co/android/]). Depending on an organization’s needs and usage context, these tools could potentially have a role to play. A small/medium business (SMB), for example, might find that the Apple Configurator fits the bill for initial hardening or that Android device manager’s basic device protection services, such as remote wipe in the event of a lost or stolen device, are sufficient for its needs without employing a heftier (read “more expensive”) solution.

5. Repurposing Mobile Devices

One area of opportunity—particularly for an SMB or severely budget-strapped organization—is the repurposing of mobile devices to accomplish other security tasks. Anybody who works in IT will tell you that one thing they tend to have quite a bit of is old, out-of-date or otherwise unused mobile devices such as decommissioned employee smartphones. Under the right circumstances, these devices can actually still provide some value to a security team. For example, there are applications that allow an Android or Apple smartphone to operate as a remote security camera. The specific app to do this varies by platform, but almost any smartphone with a camera (even if no longer connected to the cellular network) can provide video or still image data via a WiFi connection. Is this a replacement for an “enterprise-grade” monitoring capability? Of course not. But it can provide a stopgap mechanism to ensure that locations are being appropriately monitored on a short-term basis in certain situations—for example, in the interim period between when a gap in coverage is identified and new equipment is fielded or in the case of a short-term extension in coverage. Likewise, older (typically Android) devices can be used as remote wireless access point detection mechanisms in certain situations, for example, an organization with a large physical area to cover (e.g., numerous remote field offices or retail locations). There are literally dozens of free WiFi analyzers in the Android marketplace that will provide information about wireless networks in range. When used at a location where rogue access points are an issue and monitored remotely, these tools can alert to new, unexpected access points. Again, is this the ideal solution for all wireless intrusion prevention needs? Probably not. But can it make for a low-cost stopgap to help accomplish very targeted tasks such as rogue access point detection in the short term? Yes, it can—and under the right circumstances, that can be valuable.
3. What assurance does the organization have that the employees comply with the compliance- and privacy-related policies when accessing and using the organization's data?

4. What assurance does the organization have that employees back up organization-related data from personal devices?

5. What assurance does the organization have that employees will not install any unauthorized software that will compromise the organization's proprietary data?

6. What assurance does the organization have that employees will hand over their devices for investigation in case of any suspected/actual privacy breach?

Many organizations today have implemented technology to monitor employee communications to ensure that employee behavior is compliant with privacy laws, regulations and policies. These measures might particularly be required for organizations such as banks, utility providers, finance companies and listed companies that are highly regulated, especially to ensure the security of information, track insider breaches, and prevent crimes such as collusion and insider trading. The main challenge is to draw a line between organizational privacy, compliance and the personal privacy of employees.

This issue must be addressed by the policies of the organization so as to strike a balance between compliance and employee privacy.

Many organizations implement security monitoring processes using technology such as mobile device management (MDM) and security information and event management (SIEM). The features of MDM allow organizations to:

- Protect devices from unauthorized access
- Restrict the installation of applications (apps) to safeguard devices against malware
- Track the physical location of a device

**Q** Our organization has employees who work mostly in the field. Previously, they had been provided laptops and mobile phones by the organization. Now, the organization has adopted a bring your own device (BYOD) policy. The security team has implemented policies to secure these devices. The question I have is what are the privacy issues associated with these mobile teams using their own devices for the organization’s work?

**A** There are multiple aspects in this one question. Let us break down the question into small questions:

1. While allowing users to use their mobile devices for the organization’s purposes, which security settings are likely to affect their privacy?

2. What assurance does the device owner have that the organization does not monitor privacy-related information while monitoring the device for security?
• Wipe data on a device if it is lost or stolen, or if the employee leaves the company.

In other words, organizations can remotely access an employee’s devices and track the employee’s activities. Therefore, the answer to the first question is, “Yes, organizations can remotely access devices and privacy-related information.”

Monitoring of devices also answers the third, fourth and fifth questions. The organization can monitor mobile staff activities to ensure privacy-related compliance. Now, with regard to the second question, the prima facie answer is “none.” When the organization monitors devices, the organization can access the privacy-related information of the employee/device owner. As for the sixth question, the answer is none.

To overcome this situation, an organization’s BYOD and privacy policies must address it. The compliance related to privacy can be addressed by adopting the Organisation for Economic Co-operation and Development (OECD) principles for protecting privacy-related data:

• **Notice**—The organization needs to provide notice to the mobile staff that their devices are monitored for security and there is the possibility that privacy-related information may be collected by the organization. This notice should also include remote access to the device and the backup of device data that may include privacy-related information.

• **Purpose**—The organization should also inform the employees as to the objectives of remote access and monitoring, which are focused primarily on ensuring security over the organizational information contained in the device.

• **Consent**—Employees must consent to such monitoring. Some employees may refuse to comply, in which case the organization cannot monitor their devices. Of course, the organization has every right then to not allow BYOD for those employees. Employee consent should also include the handing over of their devices for investigation in case of an incident.

• **Security**—The organization is accountable for securing privacy-related information, including backup information.

• **Disclosure**—The processes of data collection, storage and disposal may be explained to the employees within the limits of the security policy.

• **Access**—Employees should be kept informed about the status of privacy-related data.

• **Accountability**—The organization is accountable for the breach of privacy-related data collected in any manner, including monitoring of mobile devices. This may be considered an extension of the principle of security. Organizations need to implement reasonable security to protect privacy-related information collected. In cases where there is a security breach resulting in leakage of privacy-related information, the organization is accountable.

• **Acceptance**—Mobile staff must be made aware of the policy and consent must be obtained before configuring the device and allowing it to be used by the employee for official business.

The monitoring of devices may be active (when a device such as a smartphone is in use) or passive (when a device is connected to the network). In either case, following privacy-related principles helps organizations monitor data usage by mobile staff.
ACROSS
1 Catchphrase for a foolhardy, expensive, security failure, 2 words
6 Many megs
8 Respond reciprocally
9 One of the steps in considering an audit program
11 Misrepresent
12 Inserted clandestinely
13 They are needed to gain access
14 Speculates
16 You can get a green belt and a black belt in these business management techniques, 2 words
20 Word used with supply and command
22 Took into account
23 New ISACA publication, Transforming ___ Security
25 Regret
26 Standards
30 Hackers now focus more on stealing these from authorized users of a system
34 Sign, as in a contract
35 It records all the activities in a system
36 Deception, often carried out in cyberspace
37 ___ it is fine, but will it work in practice?, 2 words

DOWN
1 Word used before compass or hazard
2 Chair of ISACA's Board of Directors and Inspector General of the US House of Representatives, Theresa
3 World wide web
4 Deceptive type of software
5 Converts into a particular form technically
6 Channeling
7 Techies, in slang
10 Forceful stream
12 Failing to implement these is one of the major causes of security failures
14 Kind of surge
15 That ship
16 Scientists' metric system, abbr.
17 Whistleblower
18 Top US school category
19 Broadcast
21 Explain further
23 Sources, as in a paper
24 Obstruction
27 Questions
28 Data storer
29 ISACA's charitable foundation
30 Firms, for short
31 Sense of self
32 Little toymaker
33 Reject word

Answers on page 58
TRUE OR FALSE

RAVAL AND SHAH ARTICLE

1. To address risk exposures in third-party risk management environments, host companies consider the vendor as the target of evaluation at the time of onboarding and on an ongoing basis as well. For this, the host company should implement and use both traditional and innovative monitoring approaches for continuous monitoring of the identified risk factors.

2. Agile and effective trust relationships do not rely on governance practices. Most organizations working with third parties do have a coherent plan for ongoing management of the relationship and the services that are provided. The contract and the various service agreements will be self-managing.

3. Given the complex cyber-based relationships with third parties, the new direction used to track the relevant engagement risk is dynamic risk profiling.

KRESS AND HILDEBRAND ARTICLE

4. Without a consolidated data set to analyze, the process of gathering and managing data is inherently inefficient. The absence of a coordinated, functionwide strategy led to the analytics enthusiasts having a hard time getting started and a harder time getting access to the right data.

5. Maximizing the power of analytics during the execution of the audit includes creating automated dashboards for department risk assessments and review of effectiveness of testing procedures in governance, risk and control (GRC) (control tested vs. issues noted).

6. Tomorrow’s use of analytics in the execution of an audit includes increasing horizontal review across all teams and encouraging disruption using an innovative analytical approach through custom analytics.

SMITH ARTICLE

7. Most blockchain proofs of concept are designed to achieve benefits that fall loosely into one of the three categories: reduce costs and create process efficiencies, create an ecosystem with higher-than-standard levels of trust, or facilitate digital currency exchange.

8. Ongoing review to ensure the sustainability of the assurance solution in blockchain will not be necessary, but the nature, timing and extent of the review work cannot be determined by the technology used, the business-use case and the evolving ecosystem in which the instance is deployed.

ALEXIOU ARTICLE

9. Agile audit is primarily about increasing the efficiency mainly of complex audits by parallelizing tasks, eliminating or mitigating bottlenecks, and assigning time to various tasks that is proportional to each task’s importance.

10. With regard to the audit aspect of leadership, Agile audit is more democratic, as all team members participate more or less equally (in principle) to planning.

11. Some of the Agile audit guidelines include striving to gain an early understanding of the key audit issues and disseminate this information within the audit team, discussing findings as they are gathered, and shifting resources if necessary.

PAREEK ARTICLE

12. Efforts at quantification of either black-box logic, such as modeling loss distributions based on extreme-value theory, or the combination of various security metrics (often using weighted averages) as a composite metric have been successful enough to win widespread adoption.

13. In situations where thresholds have been established, an alternative and simpler approach that relies on z-scores can be adopted. This approach is just as sensitive and precise as the standardized scores.
TRUE OR FALSE

RAVAL AND SHAH ARTICLE
1. __________________________
2. __________________________
3. __________________________

ALEXIOU ARTICLE
9. __________________________
10. __________________________
11. __________________________

KRESS AND HILDEBRAND
ARTICLE
4. __________________________
5. __________________________
6. __________________________

PAREEK ARTICLE
12. __________________________
13. __________________________

SMITH ARTICLE
7. __________________________
8. __________________________

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 by email to info@isaca.org or by fax to +1.847.253.1755. If you prefer to mail your quiz, in the US, send your CPE Quiz along with a stamped, self-addressed envelope, to ISACA International Headquarters, 3701 Algonquin Rd., #1010, Rolling Meadows, IL 60008 USA. 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.

NAME
__________________________

ADDRESS
__________________________

CISA, CRISC, CISM or CGEIT #
__________________________

Answers: Crossword by Myles Mellor
See page 56 for the puzzle.

Based on Volume 2, 2017

ISACA JOURNAL VOL 4
standards guidelines
tools and techniques

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, Thought Leadership and Research via email (standards@isaca.org); fax (+1.847.253.1755) or postal mail (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, 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.
The main purpose of ISACA Privacy Principles and Program Management Guide is to provide readers with a harmonized privacy framework. The book offers a set of privacy principles that align with the most commonly used privacy standards, frameworks and good practices, as well as fill in the gaps that exist among these different standards. This practical guide can support or be used in conjunction with other privacy frameworks, good practices, and standards to create, improve and evaluate a privacy program specific to the practitioner’s enterprise. Special guidance on how to use the COBIT 5 framework to implement a more robust privacy program is included in this publication.

How do organizations know they are effectively utilizing enterprise technology resources to best realize business goals? Do organizations know the extent to which their business goals are dependent on technology? How do they know the technology they have in place is providing value and realizing the expected return on investment?

Governance of enterprise IT (GEIT) is the systematic process of answering these and other related questions. Implementing a GEIT system can bring many benefits to an organization, including lower costs, greater control, more efficient and effective use of resources, and overall better strategic alignment and risk management. The primary purpose of adopting and using a GEIT system is to deliver value to stakeholders. This guide provides the necessary steps to implement GEIT to help the enterprise achieve its goals and demonstrate value delivery.

This guide is intended for people who are new to GEIT or have recently been tasked with implementing a GEIT structure. Whether the enterprise is already familiar with GEIT concepts and practices or is exploring the possibilities, this guide will help provide an understanding of the steps to implement GEIT and examples of the benefits of GEIT, so that buy-in from senior leadership can be obtained and a framework to guide implementation efforts can be used.
**Privacy Means Profit: Prevent Identity Theft and Secure You and the Your Bottom Line**

by John Sileo  
Product Code: 1WPMP  
Member / Nonmember: $15.00 / $25.00

Bulletproof your organization against data breach, identity theft, and corporate espionage.

In this updated and revised edition of *Privacy Means Profit*, John Sileo demonstrates how to keep data theft from destroying your bottom line, both personally and professionally. In addition to sharing his gripping tale of losing $300,000 and his business to data breach, John writes about the risks posed by social media, travel theft, workplace identity theft, and how to keep it from happening to you and your business.

By interlacing his personal experience with cutting-edge research and unforgettable stories, John not only inspires change inside of your organization, but outlines a simple framework with which to build a Culture of Privacy. This book is a must-read for any individual with a Social Security Number and any business leader who doesn’t want the negative publicity, customer flight, legal battles and stock depreciation resulting from data breach.

Protect your net worth and bottom line using the 7 Mindsets of a Spy

- Accumulate Layers of Privacy
- Destroy Data Risk
- Evaluate the Offer
- Monitor the Signs
- Eliminate the Source
- Lock Your Assets
- Interrogate the Enemy

In this revised edition, John includes an 8th Mindset, Adaptation, which serves as an additional bridge between personal protection and bulletproofing your organization. *Privacy Means Profit* offers a one-stop guide to protecting what’s most important and most at risk-your essential business and personal data. Please note that COBIT 5 Implementation Guide is also available as a complimentary web download to both ISACA members and nonmembers.

**Securing Mobile Devices**

by ISACA  
Product Code: CB5SMD1  
Member / Nonmember: $35.00 / $75.00

This publication is intended for several audiences who use mobile devices directly or indirectly. These include end users, IT administrators, information security managers, service providers for mobile devices and IT auditors. The main purpose of applying COBIT 5 to mobile device security is to establish a uniform management framework and to give guidance on planning, implementing and maintaining comprehensive security for mobile devices in the context of enterprises. The secondary purpose is to provide guidance on how to embed security for mobile devices in a corporate governance, risk management and compliance (GRC) strategy using COBIT 5 as the overarching framework for GRC.

**Security Strategies in Windows Platforms and Applications, 2nd Edition**

by Michael G Solomon  
Product Code: 3JBSS2  
Member / Nonmember: $102.00 / $112.00

Revised and updated to keep pace with this ever changing field, *Security Strategies in Windows Platforms and Applications, Second Edition* focuses on new risks, threats, and vulnerabilities associated with the Microsoft Windows operating system. Particular emphasis is placed on Windows XP, Vista, and 7 on the desktop, and Windows Server 2003 and 2008 versions. It highlights how to use tools and techniques to decrease risks arising from vulnerabilities in Microsoft Windows operating systems and applications. The book also includes a resource for readers desiring more information on Microsoft Windows OS hardening, application security, and incident management. With its accessible writing style, and step-by-step examples, this must-have resource will ensure readers are educated on the latest Windows security.
Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks

Cyber Threat! How to Manage the Growing Risk of Cyber Attacks is an in-depth examination of the very real cyber security risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. Written by one of the nation’s most highly respected cyber risk analysts, the book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences. Much more than just cyber security, the necessary solutions require government and industry to work cooperatively and intelligently. This resource reveals the extent of the problem, and provides a plan to change course and better manage and protect critical information.

Recent news surrounding cyber hacking operations show how intellectual property theft is now a matter of national security, as well as economic and commercial security. Consequences are far-reaching, and can have enormous effects on national economies and international relations. Aggressive cyber forces in China, Russia, Eastern Europe and elsewhere, the rise of global organized criminal networks, and inattention to vulnerabilities throughout critical infrastructures converge to represent an abundantly clear threat. Managing the threat and keeping information safe is now a top priority for global businesses and government agencies. Cyber Threat! breaks the issue down into real terms, and proposes an approach to effective defense. Topics include:

• The information at risk
• The true extent of the threat
• The potential consequences across sectors
• The multifaceted approach to defense

The growing cyber threat is fundamentally changing the nation’s economic, diplomatic, military, and intelligence operations, and will extend into future technological, scientific, and geopolitical influence. The only effective solution will be expansive and complex, encompassing every facet of government and industry. Cyber Threat! details the situation at hand, and provides the information that can help keep the nation safe.

Advanced Persistent Threats: How to Manage the Risk to Your Business

Advanced Persistent Threats: How to Manage the Risk to your Business explains the nature of the security phenomenon known as the advanced persistent threat (APT). It also provides helpful advice on how to assess the risk of an APT to the organization and recommends practical measures that can be taken to prevent, detect and respond to such an attack. In addition, it highlights key differences between the controls needed to counter the risk of an APT attack and those commonly used to mitigate everyday information security risk.

This book is designed primarily for security managers, IT managers, IT auditors and students studying for computer science or information security qualifications. It is written in clear, nontechnical language so it will also be of value to business managers and government officials responsible for valuable intellectual assets or critical services that might be the target of an APT attack.
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

Section two of each chapter consists of reference material and content that support the knowledge statements. The material enhances CRISC candidates’ knowledge and/or understanding when preparing for the CRISC certification exam. Also included are definitions of terms most commonly found on the exam.

CRISC Review Questions, Answers & Explanations, 4th Edition


Many questions have been revised or completely rewritten to be more representative of the 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.

CRISC Review Questions, Answers & Explanations Database - 12 Month Subscription

The CRISC™ Practice Question Database is a comprehensive 500-question pool of items that contains the questions from the CRISC™ Review Questions, Answers & Explanations Manual, 4th Edition. The database is available via the web, allowing CRISC candidates to log in at home, at work or anywhere they have Internet connectivity. The database is MAC and Windows compatible.

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.
Competition, regulation, evolving technology—change is constant. As a global leader in training, education and certification for information systems and business professionals, ISACA® can provide enterprise employees with the knowledge and skills to take on the challenges and build on the opportunities of an ever-changing world. Our Enterprise Training and Continuing Professional Education (CPE) programs are:

- Customizable to your specific needs.
- Available at or near your location, reducing downtime and travel.
- Taught by expert trainers with real-world experience.

Learn more about ISACA Enterprise Training at: www.isaca.org/enterprisetraining
Does your audit software allow you to carry key facts and insights to senior management meetings?

R-CAP™ brings Audit Universe & KPIs to your fingertips.

Audit Life-Cycle and Risk Management Solution

Observations Tracking
Risk and Controls Matrix
Regular Business Monitoring
Efficient Work-Paper Documentation
Insightful Dashboards & Reports
Resource Scheduling

Built by Auditors, For Auditors.

For your free 30 day trial email at contactus@rcap.online

www.rcap.online

Copyright 2017, Tronix Software Solutions LTD, All Rights Reserved.