Cybersecurity changes almost on a daily basis, making it quite difficult for companies to keep up. A recent study of 1,800 C-suite and other IT and information security executives by Ernst & Young found that 36 percent of organizations don’t have a threat intelligence program, and a similar percentage didn’t have real-time insights into cyber risks.

The threats that can happen come from all sides as well, both inside and outside of the company, from people doing it accidentally or maliciously. This is where internal audits can often be a helpful tool in finding weaknesses in the business processes that lead to stronger technical controls.

People see auditors as more helpful these days, Will Gosnell, director of internal audit for Gables Residential, said. It’s important that people understand that audits are not just for financial, but for all parts of the business, he added.

“Cybersecurity is evolving everyday, so it is something all of us will wind up living with,” he said. “All audit directors are challenged with updating risk assessments quarterly or once a year, so we have to put this on our radar.”

With an audit comes objectivity and hard questions, Gosnell said. Those involve going through each employee to see if they really do need that certain level of computer access — basically protecting the end users from themselves, he added.

He recalled a situation where the system administrator for a vendor wanted to give the five auditors full administrator access. “We said, ‘No, you are giving us too much,’ we don’t want the ability to change anything,” Gosnell added.

When going through an audit, the committee starts at the basic level, following a set of policies and procedures, digging into every access right from the bottom to the top, he said. If the policy is written correctly, everyone will have the right access, and often Gosnell will do a pre-test sample of 10 people to see what kind of access they have.

Most people think cybersecurity is a technology problem, and it is proliferated by tech because of the ability to be connected, but really it is a business risk with business implications, Jamie MacLean, partner in advisory services for Ernst & Young, said.

First, a company has to understand what its risk profile is — what would employees be after, what would contractors be after, what would others be after. Then determine where efforts need to be made, she added.

However, MacLean said internal auditing departments struggle with how to be connected safely. EY’s Global Internal Audit survey found that while

CONTINUING ON PAGE 9C
Balancing business risks, controls

BY DOUG DELOACH Contributing Writer

Amid significant economic uncertainty and regulatory scrutiny, executive strategists seeking new avenues for growth must become more adept at making risk-adjusted decisions that balance business value with effective internal control. To achieve this balance, internal audit experts stress the importance of maintaining thoughtful oversight and instituting meaningful controls based on proven problems rather than perceived threats.

“The tone at the top regarding risk should be appropriately balanced and stay consistent, and should always align with board expectations,” said Frank C. Beaumont, senior vice president of internal audit at Global Payments Inc.

The tendency for some stakeholders to avoid risk and others to gamble complicates the environment in which decisions must be made. The increasing size, complexity and volume of projects under consideration can also be an influencing factor.

“IT governance, risk management, and compliance are interrelated,” said Barbara Jesup, chief audit and risk executive at Duluth-based automotive retailer Asbury Automotive Group Inc. “A lot of information is digitally recorded and stored, but because of the nature of the business we are in, we also gather a lot of data manually, which means there is still a lot of paperwork.”

Best advice to clients:

▶ Internal auditors are more interested in helping management improve its control environments rather than simply finding errors and assessing blame.
▶ It’s OK to request that the audit process draw attention to a particular operational deficiency, which could benefit from management attention or additional resource allocation.
▶ Know where your valuable assets (e.g., software, information, financial assets) are, and who has access to them.
▶ Engage internal audit early in projects and key operational changes. Better to identify and address governance, risk, and control concerns up-front, before a significant investment of time and money.
▶ Follow up on action plans resulting from an audit and make sure they are fully implemented.

The project audit space has become more challenging with the increased complexity and scale of projects, particularly IT projects,” said Brian Bowling, chief audit executive at the Federal Reserve Bank of Atlanta. “Tension can arise when stakeholders apply traditional organizational risk tolerances for core operations, which they understand well, to large projects that have a different set of risks.

At the outset of a major multi-year project, when a lot of unknowns are present, Bowling said stakeholders need to weigh their tolerance for uncertainties against the cost of avoidance if a project is not undertaken. The tendency to avoid risk may result in “foregoing better operating efficiency, customer service capabilities, and technological functionality in the future.”

Compounding the inherent uncertainty associated with a new venture is the heightened awareness of the consequences of failure caused by ineffective controls, which is more acute today in the shadow of high-profile financial scandals. From Bernard Madoff’s Ponzi scheme, which bilked investors out of billions, to the global Libor scandal of 2013, not to mention the fraud, embezzlement and corruption headlines surrounding companies like Enron and Arthur Anderson, the spotlight on corporate financial malfeasance has never been brighter.

“When I see headlines about corruption and fraud, it always triggers a discussion with my audit team about our own controls and whether it could happen in our environment,” Bowling said.

Standard operating procedures for Bowling’s team calls for routine testing and follow up on action plans resulting from an audit and make sure they are fully implemented.

Risk management helps bottom line

BY GARY A. WITTE Contributing Writer

It’s a trend that continues to see their auditors as something to plan with — not just to hunt down problems.

The shift in attitudes has come gradually during the past decade, if not longer, according to auditing professionals.

Ric Kimball, principal of the audit and tax advisory firm KPMG LLP, said the days of reactive auditing are going away. Continuous risk assessments are becoming the norm. Companies are including auditors more in strategic planning and using their input about new technologies, new products and emerging risks.

“I think it’s an evolution,” Kimball said. “We’re being asked for more.”

For instance, cybersecurity was previously just the job of information technology professionals, but now auditors often help determine what the company should do in the event of an Internet breach, he said.

“There’s a lot of proactive activity taking place,” Kimball said. “You now have to look not just can you do it, but what if they do. What is the response if an event transpires?”

In order to accommodate these responsibilities, auditor offices are becoming more diversified.

Lori Kaczynski, chief audit executive for Printpack Inc., said a good internal audit office should be connected with key departments at all levels of the company and auditors need a broad base of knowledge to accomplish their work.

“When we have to know has exponentially grown,” she said. “We’re not auditors anymore. We need to consider ourselves business partners.”

A 2013 survey of chief audit executives by Ernst & Young and Forbes Insights said 28 percent believed internal auditors played a strategic role, but 54 percent expected the role of “strategic adviser to become the profession’s primary mandate.

The same percentage of the executives said auditors to be heavily involved in identifying, assessing and monitoring emerging risks.

72 percent of executives said they expected the auditors to complete a separate emerging risk assessment.

Source: 2013 survey by Ernst & Young and Forbes Insights

Closser look

54 percent of chief audit executives surveyed expect the role of strategic adviser to become the profession’s primary mandate.

The same percentage of the executives said auditors to be heavily involved in identifying, assessing and monitoring emerging risks.

72 percent of executives said they expected the auditors to complete a separate emerging risk assessment.

Source: 2013 survey by Ernst & Young and Forbes Insights

The thing I always encourage my employees to do is get out of their chairs and talk to people,” Gensler said.

Working closely with other sections also has the benefit of seeing the auditors as part of the team and help change the culture of the company for the better, she added. Some people are afraid to talk to auditors because they don’t want to look bad.

“I think it’s trending towards them thinking of you as more of a business partner, but you’re always going to have those people who think of you as the police,” Gensler said.

Internal audit helps ensure internal controls of a business and helps prevent errors, but can also save the company’s reputation and assets. As a troubleshooter, auditors can help companies better manage risk, she said.

“You’re trying to prevent anything from happening in the future,” Gensler said.

Through operational reviews, auditors can also check efficiencies and see if the company’s money is being spent effectively.

For example, a review of a product order process might discover redundancies and waste that reduce profits and slow delivery times, she said.

“Instead of entering a sales order three times, you enter it one time,” Gensler said.

Kaczynski said many businesses are looking for ways auditors can add more value to the company and have begun to understand the financial benefits of having them.

“We’re getting that request at all levels,” she said. “I think we’re definitely moving towards the good end.”
The Internal Audit Center is privileged to have an Advisory Board comprised of members whose wisdom and guidance is extremely valuable and most appreciated as the Internal Audit Center evolves.

“I decided to pursue a one-year full-time Master of Accounting program at KSU. I take advantage of as many opportunities as I can now, such as the Internal Auditing Education Partnership Program’s Networking Retreat, other events at KSU, and in our MAcc program.”

NITZAN AUZ
KSU MAcc Class of 2015
The Institute of Internal Auditors
January 2015 Rising Star

MAcc Students Joseph Nerbonne, Bindia Mathew, Shannon Collins, and Brian Gelfand represented the Kennesaw State University Master of Accounting Program (MAcc) at the 2014 IAEP Leadership Conference.

The Institute of Internal Auditors
January 2015 Rising Star
Growing use of data among future expectations

BY NICOLE BRADFORD
Contributing Writer

Each year, business analytics and information services firm PRGX processes about 2.4 million client files, analyzing more than 1 trillion client transactions.

Founded 40 years ago, the Atlanta-based company’s clients include some of the world’s top global retailers, for whom it secures and analyzes increasing amounts of data for financial insights.

“Yes, we’ve got to have strong IT and data analytic skills, as well as the education behind it, he said. “There are certifications we look for, and strong problem-solvers with critical thinking abilities.”

A new job description gaining traction among future expectations for IT auditors.

“Instead of a three-day class, we work with them over the course of a month or two and do a project together,” he said.

The analytics method is a much more complex technique than what is traditionally used, Oringel said, because internal audit professionals are not usually programmer-data types.

“internal auditing,” he said. “We have developed some proprietary software and means of getting data from clients in a way that is secure and that enables us to process this data, cleanse it and do all kinds of things with it,” Masci added.

With big data comes big responsibilities. A fast-growing pool of data poses both risk and new opportunities for organizations that generate and store it.

“When you have a lot of data, that causes a lot of concern for data security, and that’s where the internal auditing comes in,” Masci said. “It requires skill sets that 10 to 15 years ago did not exist.”

Cybersecurity – once an issue people though applied only to banks – is a valid concern for all companies, and internal audit plays a key role in developing and testing internal controls, he said.

“In our own company, we have our own data that we’re concerned about, but we also have a massive amount of client data. We cannot have anything happen to that data. We have to completely secure it,” he said.

Dealing with such challenges, he said, requires finding people with skills that are fairly scarce today. Masci said his colleagues often comment on the rising demand for IT auditors.

“You’ve got to have strong IT and data analytic skills, as well as the education behind it,” he said. “There are certifications we look for, and strong problem-solvers with critical thinking abilities.”

A new job description gaining traction – and in much demand – is that of data scientist.

“I have an internal auditor who already has a master’s in accounting, now getting a master’s in statistics,” he said, “and utilizing data mining tools and techniques so we can explore large amounts of data.

The internal auditor of the future wants to look at 100 percent of the population, not just a sample.”

Experts believe that data analytics – finding meaningful patterns within large amounts of data – will continue to make its way onto the audit departments’ to-do lists.

For many companies, though, there remains a gap between planning and talking about the benefits of using data analytics and actually employing it.

“Internal analytics makes organizations not do effective use of their raw data to make business decisions,” states Masci.

Vast amounts of data stored by organizations has always presented an opportunity for internal audit departments to test controls, monitor compliance and drive strategic insights more efficiently and effectively, said Julie Hower, senior director of internal audit and enterprise risk management at Carter’s Inc.

“I, in my opinion, at this time most organizations do not make effective use of their raw data to make business decisions,” states Masci.

While data analytics creates efficiencies, it may not be realized initially, as there is an investment in time to stand up these new techniques vs. ‘doing it the way we’ve always done it,” she said.

Internal auditors strive to serve as advisers and predict risks before they emerge, she said.

“Leveraging vast amounts of data to drive innovation and reduce risk is a necessary competency for internal auditors, in my opinion, so that we can continue to demonstrate our value to the organization,” said Hower, who now staffs her team with those holding both CPA and CISA, or Certified Information Systems Auditor, certifications, along with data analytics experience.

The realm of analytics involving continual protection of a company’s resources through monitoring of internal functions is a specialty of consulting and service firm Visual Risk IQ. Through what Partner Joe Oringel calls an “apprentice model,” the company works with organizations to use analytics to establish accurate and continuous internal controls.

“Data analysis is important,” Oringel said, “and it’s difficult, but if you do it right, it pays wonderful dividends and makes the audit department look like heroes, because they are looking at everything, and finding things they wouldn’t find if they just looked at a sample. If you want to see if employees are charging the right amount for breakfast or dinner and keeping with company policy, you can go to the paper files and look at 20 or 30 and do it all by hand, but a large company has thousands of travelers doing multiple expense reports per month. The best way to do that is not to pick 25 and check them, but load all the data associated with travel into a second program.

Audit analytics is auditing with a computer, using the computer to analyze all transactions as opposed to a sample, he said. “I would say that analytics is the opposite of sampling.

The apprentice model used by the company includes working side-by-side with staff on an audit procedure.

“Instead of a three–day class, we work with them over the course of a month or two and do a project together,” he said.

The analytics method is a much more complex technique than what is traditionally used, Oringel said, because internal audit professionals are not usually programmer-data types.

“You need internal auditing and data skills to be successful in this sub-field of internal auditing,” he said.

Changes in expectations from regulators, investors and the public may soon require that data analysis and visual reporting be used much more widely in the internal audit profession, Oringel said.

“We all generate huge volumes of data,” Oringel said. “But turning that data into information, and then making good decisions with that information is why data scientists are among the top 10 jobs of today.”

Masci agreed.

“You want folks who can really gather the information, cleanse it, reform it and transform it into something that is smart data as opposed to raw data,” he said.

“One of the key, it is in a format, you can glean insight from, that’s where critical thinking and problem-solving comes in. It’s amazing where internal auditing is going.”

Top in-demand skills for IT auditors

- Strong IT and data analytics skills and education
- IT auditing certification such as CISA (Certified Information Systems Auditor) or CISSP (Certified Information Systems Security Professional)
- Problem-solving ability and critical thinking skills
- Excellent verbal and written communication skills
- Experience with a wide range of computer systems and security and data tools
- Business acumen
- Flexibility and ability to multi-task in a fast-paced environment

Source: Fred Masci, PRGX
Several years ago, I wrote, “Fraud is a human endeavor, involving deception, purposeful intent, intensity of desire, risk of apprehension, violation of trust, rationalization, etc. So, it is important to understand the psychological factors that might influence the behavior of fraud perpetrators. The rationale for drawing on behavioral science insights is evident from the intuition that one needs to ‘think like a crook to catch a crook.’”

Because the human factor in fraud is paramount, internal auditors must add the emerging field of behavioral forensics to their knowledge base.

Behavioral forensics relies primarily on psychology to understand the behavioral/integrity risks and the behavioral dynamics that may lead to fraud. Fraud frequently involves emotional manipulation, including big and small lies and deliberate misrepresentations made by the perpetrator.

Fraudsters earn the victim’s trust, only to violate it. The psychology of several interacting parties is also pertinent: the psychology of the fraud perpetrator(s), the psychology of the victim(s), the psychology of managers and auditors, the psychology of regulators, the psychology of whistleblowers, if any, etc.

The “why” of fraud – why “good people do bad things” – may involve a multitude of reasons, e.g., noble cause corruption, revenge fraud, fear/pressure to preserve status and wealth, keeping parity with others, playing a catch-me-if-you-can game, avoiding shame, etc. Interestingly, incompetence in managing shame and pride, two important and powerful emotions, may unwittingly lead people to commit fraud. Narcissism, or excessive pride, could lead one to cross the line, and the shame of not have accomplished anything significant by mid-career, may compel an irrational urge to do whatever it takes to “show the world.”

Fraud is frequently a team sport. The bad apple, or rogue executive, frequently recruits others to make it a collusive act.

Where there is dysfunctional leadership, and a toxic culture in the organization, the resulting bad crop scenario can encourage rampant, unethical behaviors. We are learning more about “accidental fraudsters” (those who find a hole in the systems, exploit it, like the result, and stay on the wrong side of the ethical line) and “predators” who are the natural born crooks, the sharks, and prey on their gullible victims.

Internal auditors are required by The IIA’s International Standards to have “sufficient” knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization. In addition to putting in place strong internal controls, organizations may have designed and communicated a code of ethics and values, set up ethics and whistleblower hotlines, and carefully gone about setting and communicating the proper tone from the top.

More knowledge and training in human behavior – a complex topic – can increase internal auditors’ professional skepticism. Evaluating the climate of ethical behavior, perhaps by carrying out ethics and culture audits, is becoming the norm in the new era of corporate governance.

More importantly, internal auditors need the “moral courage” to speak truth to power when they may, on occasion, discover senior executives engaging in questionable behaviors and/or fraudulent conduct – referred to by one lawyer as the “wicked problem of C-suite misconduct.”

Mastery of behavioral forensics concepts will greatly aid them in helping their organizations become fraud resistant – by promoting a culture of integrity where fraud becomes an unattractive option, and successfully achieve a culture of compliance and fraud deterrence.
Social media: With great risk comes great reward

BY PHIL W. HUDSON
phudson@bizjournals.com

Social media can be a risky way for companies to promote products and services, communicate with customers and build brand reputation, but “with great risk comes great reward,” said one major Georgia company executive.

To help determine if a company’s social media strategy is worth the risk, several companies use auditors.

Sabrina Serafin, partner with the process, risk and governance group at the Atlanta-based CPA firm Frazier & Deeter LLC, said as an auditor, the way she approaches social media is on the risk assessment level.

“As auditors, we use the terminology of mitigating the risk, so how do we get comfort when we understand that social media is part of the environment? It’s first identifying and monitoring the reputational risks,” Serafin said.

“Not including social media risks in the overall organization’s overall risk assessment is something that auditors would be concerned about and would want incorporated into the overall risk management program.”

Serafin added that risk management programs that identify, measure and monitor social media are based on the size and complexity of the company and how involved it is in social media.

“I’m sure there are some companies that would argue they wouldn’t exist without it, so the risk management program is going to look very different than say a manufacturing company that encourages users to post when there’s a new product or upgrade, something that would go well being communicated through that type of medium,” Serafin said. “But, you have to take into consideration any kind of regulations that may impact an industry, the organization and the type of data that a company is involved in. An example would be a financial services firm or a health-care provider where you have financial data or personally identifiable health identification because that data has to be very much protected. And when you have someone who is maliciously or unintentionally posting information that could violate a governmental agency’s requirements or regulatory requirements, the organization is open for potential litigation or negative attention.”

Serafin said auditors should understand who owns the social media process in addition to making sure that management understands the risks and act as intermediaries to make sure those risks are mitigated.

The way external and internal auditors can mitigate risk is by making sure that the individuals who are charged with using and supporting social media technology are all on the same page, she said.

That means the policies and procedures are documented, communicated and enforced within an organization, Serafin said.

“So, if we’re using social media tools,” she said, “we need to make sure that the IT department has the appropriate anti-virus applications for any mobile devices that are used, make sure teams are properly trained on the use of these tools to further an organization, and really make sure management and IT has a strategy that supports social media so the technological risks are mitigated.”

Another risk that can impact a company’s bottom line is that social media allows grievances to move from the traditional internal complaint departments to the public domain.

“There can be a potential loss to reputation for an organization or product because users have control over what is said about a company and there is not much filtering out there,” she said.

“Another financial risk is information leakage like trade secrets or information about a product that is coming internally prematurely that could undermine an organization’s marketing or sales strategy. Then there is a financial cost to repair any kind of damage and recover from an incident that stems from social media.”

One major Georgia company that uses social media for marketing and communication is Columbus, Ga.-based insurer Aflac Inc. The company has corporate Facebook, Twitter and LinkedIn accounts in addition to a Facebook and Twitter account for its Aflac duck mascot.

Aflac Inc.’s duck mascot has its own Facebook and Twitter accounts.

Alex W. Stephanouk, internal audit executive of Aflac, said Aflac uses metrics to determine the amount of “buzz” it is creating by counting website views and click-through rates.

“We want to see that [our social media] has a purpose and is trying to achieve something within measuring success, but to come in with anything that might suggest we do less in terms of social media, to me, would be like kind of like coming in several years ago and saying ‘We need to be careful about how we use email,’” Stephanouk said. “It’s sort of an embedded part of doing business today, so we’ve got to embrace and accept it and help [social media users] think through the risks to make sure they are managing those risks properly rather than trying to be their adviser and getting everything you could out of it.”

Stephanouk said when it comes to social media from an audit perspective; he is very process-focused, as the key risk for Aflac is brand reputation.

“It’s not just the accounts we have today, it’s about somebody opening other accounts that use our brand,” he said. “It could be as innocuous as the Aflac softball or somebody creating a fictitious use of the brand or an unauthorized use of the brand in a negative way and we have to make sure those things are governed. Then, we also have employees that we have to be cognizant of, and we have to balance the legal aspects of what people are allowed to do with free speech and we want to make sure we give people the tools to make sure they know what they should be doing as good stewards of our company.”

Stephanouk said Aflac collaborates with an external company about its social media use. “We want to make sure there is a documented strategy where you can tell we have a plan going into any endeavor and that there is a designed and developed process associated with that,” he said. “For us, we’re using an external firm for a lot of that design and development but then that rolls back through our organization for review and approval before it actually goes out into the public, which you would expect with any process out there.”
Internal auditors focus on today’s business risks

BY TONYA LAYMAN
Contributing Writer

Over the past decade, the role of the internal auditor has expanded to include more identification of risk that can impact business strategy and direction. As that trend continues, a number of Atlanta’s top internal auditors are helping their organizations create cybersecurity policies, combat fraud and deploy tools that result in data-driven insights.

“Just providing assurance on the financials or assurance on compliance of certain regulations is not enough. Internal audit can and should be doing more,” said Paul Sobel, vice president and chief audit executive at Georgia-Pacific LLC.

“Because of our training, experience and access to all parts of the business, we can provide assurance and advice to help enable value creation. A company is successful when it can create value. And while most people don’t think of internal audit creating value because we aren’t the decision makers, we can help management make those decisions and to be successful.”

Sobel said as cybersecurity becomes a bigger issue for corporations, it is essential that internal audit be appropriately and accurately engaged in the execution of that policy.

“Another issue that can be related to, but is not limited to, cybersecurity, is crisis response,” Sobel said. “It is imperative that you react to a crisis as appropriately and timely as possible.”

Terry Thompson, MARTA’s assistant general manager of internal audit, said he is focused on various business functions for the transit authority, but those things that are top of mind revolve around cybersecurity and fraud.

“It seems like the bad guys are constantly ahead of the good guys in this area and given the fact that we at MARTA transport people we have to maintain our ability to run our trains and buses,” he said. “There are also concerns around our ability to protect our general computer system and management reporting.”

His department has worked diligently with MARTA’s IT department to perform a comprehensive audit of the network’s perimeter security and worked to identify ways to implement appropriate strategy, infrastructure and employee training.

“We are not only looking at the short term,” Thompson said. “We have to make sure we have a sustainable program to monitor the threats and make sure the system is in place to protect us from threats. It is not one and done.”

Additionally, fraud is a source of concern for the organization.

“That is true for any organization, but at MARTA we have a lot of assets and there is a lot of opportunity for theft to occur.

We have to make sure the employees conduct themselves in a way that is honorable and respectful and that we maintain the public’s trust,” Thompson said.

MARTA has implemented the “Is it Worth It?” fraud campaign, complete with a fraud hotline and a mobile app that allows both employees and customers to take a picture and send it anonymously to police when they suspect fraudulent activity.

Sobel believes “big data,” can be used by internal audit to source business intelligence that can help drive business strategy. “We can enhance business decision-making by using tools to better perform our audits or in our analysis acumen to help drive company strategic,” he said. “We need to embrace that technology to do our jobs better and be seen as more strategic.”

Leveraging tools that can provide data-driven insights, specifically related to compliance, supply chain optimization and retail store performance, is a huge priority for Julie Hower, senior director of internal audit and emerging risk management at Carter’s Inc.

“You can use that to drive strategic insights and change,” she said, adding this information can assist the end user in identifying opportunities related to supply chain, cost reduction and retail performance.

Another priority for Hower is data privacy, cybersecurity and incident response planning and international expansion.

“As we continue to see the economy rebound, companies are more rapidly pursuing expansion initiatives,” she said. “Internal auditors, who have a strong partnership with the business and an existing seat at the table earned through demonstrated value, have the ability to play an active role in strategic decisions.”

Additionally, Hower works to align enterprise risk management activities with the evolving regulatory and compliance landscape, global macroeconomic trends and the company’s strategic priorities, while building and sustaining a team of highly skilled auditors with financial, technology and industry-specific operational expertise.

“The internal auditors market is booming in Atlanta right now and there is strong competition for talented resources especially those professionals with an IT background. It makes it challenging to find the right people and you want to make sure you provide opportunities to the team to work on a little of everything. You want them to get exposure to all facets of the business, not just the financial aspects.”

Looking ahead, Sobel believes internal auditors should be tapped as more companies deploy reporting beyond the financials. A growing number of U.S. organizations are releasing sustainability reports indicating how they are good stewards of the environment or community.

Integrated reporting which communicates the organization’s strategy, governance, performance and prospects to stakeholders is another area of reporting gaining in popularity. With both of these, internal audit should be called upon to provide assurance, he said.
# ATLANTA’S TOP 25 ACCOUNTING FIRMS

**RANKED BY NUMBER OF PROFESSIONALS IN ATLANTA**

<table>
<thead>
<tr>
<th>Business name / Prior rank</th>
<th>Address Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deloitte LLP ① deloitte.com</td>
<td>191 Peachtree St. NE #2500</td>
</tr>
<tr>
<td>EY ② ey.com</td>
<td>55 Ivan Allen Bl. #1000</td>
</tr>
<tr>
<td>PwC ③ pwc.com</td>
<td>1075 Peachtree St. NE Atlanta 678-419-1000</td>
</tr>
<tr>
<td>KPMG LLP ④ kpmg.com</td>
<td>301 Peachtree St. NE Atlanta 623-3200</td>
</tr>
<tr>
<td>Habif, Argoti &amp; Wynne LLP ⑤ haawpa.com</td>
<td>5 Centennial Pkwy.</td>
</tr>
<tr>
<td>Grant Thornton LLP ⑥ grant Thornton.com</td>
<td>1100 Peachtree St. NE Atlanta 6130-2000</td>
</tr>
<tr>
<td>Frazier &amp; Deeter LLC ⑦ frazierdeeter.com</td>
<td>121 Peachtree St. NE #1150</td>
</tr>
<tr>
<td>Bennett Thresher LLP ⑧ btlpa.net</td>
<td>3625 Cumberland Blvd. #1000</td>
</tr>
<tr>
<td>Dixon Hughes Goodman LLP dhgpa.com</td>
<td>191 Peachtree St. NE #1070 Atlanta 677-575-8800</td>
</tr>
<tr>
<td>CohnReznick LLP ⑨ colorus.com</td>
<td>5150 Lenox Rd. Atlanta 30326 404-347-9447</td>
</tr>
<tr>
<td>Cherry Bekaert LLP ⑩ cb.n</td>
<td>101 Peachtree St. #2200</td>
</tr>
<tr>
<td>Windham Brannon P.C. windhambrannon.com</td>
<td>3630 Peachtree Rd. NE #4660 Atlanta 677-248-2000</td>
</tr>
<tr>
<td>AGH LLC ⑪ agllc.com</td>
<td>3100 Piedmont Rd. #1500 Atlanta 677-3047 404-231-5486</td>
</tr>
<tr>
<td>BDO ⑫ bdo.com</td>
<td>110 Peachtree St. NE #700 Atlanta 30308 404-688-6894</td>
</tr>
<tr>
<td>Smith &amp; Howard P.C. ⑬ smith-howard.com</td>
<td>271 1117 St. NW 2#200 Atlanta 677-247-2444</td>
</tr>
<tr>
<td>Moore Colson ⑭ moorecolson.com</td>
<td>1640 Powers Ferry Rd. #11, #130 Marietta 30067 770-489-0026</td>
</tr>
<tr>
<td>Rödli Langford de Kock LLP ⑮ rdlk.com</td>
<td>225 Peachtree St. NE #1100 T. Tower Atlanta 30303 404-525-2600</td>
</tr>
<tr>
<td>Moore Stephens Tillier LLP ⑯ mstll.com</td>
<td>780 Jefferson Ferry Rd. #1335 Atlanta 677-244-3842</td>
</tr>
<tr>
<td>Carr, Riggs &amp; Ingram LLC cri.com</td>
<td>4360 Chamblee-Cleveland Rd. #3040 Atlanta 30341 770-457-6406</td>
</tr>
<tr>
<td>Mauldin &amp; Jenkins LLC mjcpa.com</td>
<td>200 Galleria Pkwy #1700 Atlanta 677-955-4600</td>
</tr>
<tr>
<td>HLB Gross Collins P.C. hbgrosscollins.com</td>
<td>3330 Cumberland Blvd. #900 Atlanta 30318 404-433-1711</td>
</tr>
<tr>
<td>Crowe Horwath LLP crowehorwath.com</td>
<td>3392 Peachtree St. NE #2700 Atlanta 677-254-1600</td>
</tr>
<tr>
<td>McGladrey LLP mcgladrey.com</td>
<td>1230 Peachtree St. NE #1700 Atlanta 677-451-8100</td>
</tr>
<tr>
<td>Porter Keade Moore LLC pkm.com</td>
<td>235 Peachtree St. NE #1100 Atlanta 677-3048-4200</td>
</tr>
<tr>
<td>Pershing Yoakley &amp; Associates P.C. pryapc.com</td>
<td>3424 Peachtree Rd. #700 Atlanta 677-3036</td>
</tr>
</tbody>
</table>

1 A professional is defined here as one required to have continuing education hours. All figures are current as of February 2015.
2 Company submitted a statement of verification supporting figures.
3 Firm headquarters and Managing partner(s) in Atlanta Year est. in Atlanta

**SOURCES:** Atlanta Business Chronicle research and the firms
I n today’s digital age, companies are becoming increasingly dependent on technology to run their business. And, as a result, companies are also becoming more vulnerable to data theft by hackers.

Constantly, you are reading headlines of companies from every industry and every size falling victim to digital theft. Who is at risk for cyberattacks? Everyone from the government to businesses to individuals is at risk. Take for example NSA and former contract employee Edward Snowden. He used a computer thumb drive to smuggle highly classified documents out of an NSA facility.

Or, in the case of Sony, the cyberattack was an intrusion into Sony’s network and consisted of the deployment of destructive malware. This resulted in the theft of propriety information as well as employees’ personal information and confidential communications.

And, in Target’s massive breach, hackers stole credit card numbers and personal data of millions of its customers.

Who is next seems to be the million (or should I say, billion) dollar question. Cybercrime has become a virtual weapon bent on compromising their victims’ IT infrastructure, for illegal gain such as corporate secrets, money or identity thefts, with no regard to borders – physical or virtual.

What are business implications of a cyberattack?

In the NSA situation, national security secrets were released and some said put CIA agents lives at risk because of blown covers.

For Sony, the cyberattacks rendered thousands of computers inoperable and forced Sony to take its entire network offline. This resulted in a significant disruption of the company’s operations. And, as for Target, millions of customers’ credit card and identities were stolen resulting in loss of sales, management turnover and even activist investors questioning the audit committee members of the board.

In addition to financial loss, cyberattacks are causing companies with otherwise good brands to lose their reputation. What role can internal auditors play in preventing a cyberattack?

To reduce the risk of a cyberattack, businesses must have policies and procedures in place for cybersecurity. And, internal auditors can play a critical role in this area. There are many definitions of cybersecurity, and here’s one from techopedia. “Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malware.”

Most internal audit dDepartments have dual roles reporting to both management and the audit committee. And, both reporting structures can help with cybersecurity concerns.

Towards management, internal auditors must measure the effectiveness of management’s cybersecurity controls. As a starting point, internal audit should ensure that organizations have sound governance and standards in place with respect to cybersecurity. This would include things like an empowered information security officer and an adopted framework that allows for common information security procedures and a common IT language across the organization.

And with respect to audit committees, they are asking what management is doing to protect their company and how do they know their efforts are effective. And, should there be no breach, does management have a response plan, and has it been tested.

Without regard for cybersecurity, company reputations are on the line. And, cybersecurity failures are visible and can negatively impact company sales, senior management, strategic alliances, and stock price, among other things.

Since the systems we rely upon now impact the entire organization and every business process, internal audit is rising to the top in terms of importance in the eyes and ears of the audit committee.

The National Association of Corporate Directors advises audit committees to be receiving updates from management and internal auditors about the following:

- Understanding and approach to cybersecurity
- Legal implications
- Access to experts
- Staffing and budget
- Risk avoidance

What is IIA Atlanta doing for its members related to cybersecurity?

IIA Atlanta is changing the focus of our monthly meetings to assist members with Continuing Professional Education and our members are responding. For example, at our most recent meeting, Ernst & Young LLP presented two one-hour topics on Cyber Economics and Internal Audit of Cybersecurity. Also, Frazier & Deeter presented on internal audit’s role in cybersecurity. The presentations were rated outstanding and we saw a 40 percent increase in attendance. For IIA Atlanta, cybersecurity has become the best thing for attendance at our Continuing Professional Education meetings since the Sarbanes-Oxley Act of 2002.

Cybersecurity issues will continue to be an important topic across all businesses. And, internal auditors will need to lead the charge to push for internal standards to reduce the risk. As the digital age propels on, The IIA will continue to educate our members on cybersecurity.

CONTINUED FROM PAGE 1C

cybersecurity was a Top 2 emerging risk, one of the skills most lacking among auditors was technology skills, understanding the level of risk and how to deal with it, she said.

“The whole thing is a complicated problem,” said Kelly Bissell, global cyber leader in risk services for Deloitte & Touche LLP.

And there’s a challenge to getting everyone on the same page. Most cyberpeople aren’t familiar with the business processes of how the company works – like how it makes money – to effectively find cracks in the system, he said. On the business side, they need the cyber people who have that different perspective, Bissell added.

“No one is going to be without something, and we are trying to anticipate weaknesses instead of discovering them,” he said. “Those emails can get really clever. It is not just the typical ones about winning a prize, but they can be received on your computer.”

After the company makes those decisions, they also need to evaluate what they need to spend, and weigh those costs with the expected benefits, Bob Scalise, senior manager of IT risk and transformation at Ernst & Young, said.

In addition, companies need to educate employees on not just all of the things that could happen, but how to use that device from home in the work environment, Bissell said. And vice versa, how employees should use their work computer at home. “Be skeptical about what could happen, and build the right controls for that.”

William Mulcahy is president and CEO of Mulcahy Consulting, and board member of IIA Atlanta, including chairman of the board 2006 – 2010.
Mitigate the risk of interdependence

BY JANET JONES KENDALL
Contributing Writer

If you are a successful business owner whose business has grown, chances are you can no longer run your company without depending on other companies to help you out — whether they run your payroll, distribute your product or operate your website.

Welcome to the world of marketplace interdependency.

The trend of marketplace globalization and interdependency has come far in the last 10 to 20 years and isn’t expected to slow down any time soon, according to Curtis Fields, a finance executive with experience as a chief audit executive, operating unit CFO and COO in technology, software and service-related industries.

“The world is becoming a more and more interconnected place; companies are becoming more and more global,” said Fields, secretary of the Institute of Internal Auditors Atlanta chapter. “If you’re local, you’re probably going regional. If you’re regional, you’re probably going national. If you’re national, you’re probably going global. I think as a result the interdependency trend continues and, if anything, accelerates.”

The three primary areas of interdependency are in a company’s supply chain, data/systems and in its outsourcing of business processes, Fields said. That’s because most marketplaces no longer have the option to operate exclusively from one another; businesses increasingly rely on interconnected webs of stakeholders to drive performance, and new technologies have made companies both hyper-connected and hyper-transparent. These relationships make businesses vulnerable for attacks from hactivists, disruptions caused by third-party breakdowns in compliance or safety, and potential public perception nightmares — all factors that increase business risks, systems risks and enterprise risks for the business, according to Fields.

The biggest risk a company takes when forming dependencies on outside sources is not understanding the full details and risks associated with how partners can disrupt or slow down the business, according to Deidra DenDanto, IIA Atlanta board member and practice director of finance and accounting consulting services for The Intersect Group.

“Completeness, accuracy and timeliness are critical to maintain our integrity with our clients so our partner provider performs a critical task on our behalf,” DenDanto said. “If there are errors, delays or irregularities in this process, it can create critical disappointments or failures with our clients as well as with our candidates, which would detrimentally impact how we are perceived and how successful we could be in the marketplace.”

Those connected, interdependent relationships will only grow in the next decade, DenDanto said, as organizations focus on core business activities and use partners for all else to save on cost and investments in non-core activities.

CLOSER LOOK

Deidra DenDanto, Institute of Internal Auditors Atlanta board member and practice director of finance and accounting consulting services for The Intersect Group, shares tips for strengthening interdependent business relationships:

1. Know your partners. Have a deep relationship that is well-managed with the appropriate governance mechanism to monitor performance, identify issues and handle problems quickly if they arise.
2. Develop a long-term deep relationship to ensure ongoing success.
3. Fully understand roles and responsibilities as well as defined business requirements and have controls over pass-offs.

The Intersect Group, IPMA Atlanta chapter: “If you’re looking for all else to save on cost and investments, strengthen interdependent business relationships that are well-managed and are becoming more and more global,” said Fields, secretary of the Institute of Internal Auditors Atlanta chapter. “If you’re not adequately qualified, you’re going to drive risk.”

Mitigate the risk of interdependence

FASTEST-GROWING ACCOUNTING FIRMS BY PROFESSIONALS

RANKED BY THREE-YEAR PERCENT CHANGE IN ATLANTA PROFESSIONALS

<table>
<thead>
<tr>
<th>Business Name</th>
<th>Address</th>
<th>Three-year % change of Atlanta professionals1</th>
<th>Number of Atlanta professionals1</th>
<th>Number of Atlanta CPAs</th>
<th>Number of Atlanta partners</th>
<th>Total full-time Atlanta staff</th>
<th>Partial listing of specialty services offered</th>
<th>Firm headquarters</th>
<th>Managing partner(s) in Atlanta</th>
<th>Year-end in Atlanta</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>McGladrey LLP</td>
<td>1230 Peachtree St. NE #1100</td>
<td>Atlanta, GA 30309</td>
<td>404-721-5100</td>
<td>253%</td>
<td>60</td>
<td>17</td>
<td>4</td>
<td>64</td>
<td>audit, tax consulting and compliance, risk advisory, financial advisory</td>
</tr>
<tr>
<td>2</td>
<td>Hancock Askew &amp; Co. LLP2</td>
<td>275 Scientific Dr. Norcross, GA 30092</td>
<td>770-397-1500</td>
<td>140%</td>
<td>24</td>
<td>13</td>
<td>4</td>
<td>26</td>
<td>audit, assurance, tax, advisory transaction and due diligence, small business and advisory</td>
<td>Norcross, GA</td>
</tr>
<tr>
<td>3</td>
<td>Carr, Riggs &amp; Ingram LLC</td>
<td>4500 Chamblee-Dunwoody Rd. #420</td>
<td>Atlanta, GA 30341</td>
<td>770-457-6000</td>
<td>132%</td>
<td>65</td>
<td>42</td>
<td>13</td>
<td>74</td>
<td>audit, tax, consulting, M&amp;A services, IT audit, retirement plan audit, manufacturing</td>
</tr>
<tr>
<td>4</td>
<td>Dixon Hughes Goodman LLP</td>
<td>191 Peachtree St. NE #7200</td>
<td>Atlanta, GA 30303</td>
<td>404-275-0000</td>
<td>66%</td>
<td>183</td>
<td>80</td>
<td>25</td>
<td>195</td>
<td>assurance, federal, state, local and international tax compliance and advisory, healthcare consulting, real estate services</td>
</tr>
<tr>
<td>5</td>
<td>Novogradac &amp; Co. LLP3</td>
<td>2325 Lawrence Pkwy, #450</td>
<td>Alpharetta, GA 30009</td>
<td>770-867-3333</td>
<td>61%</td>
<td>45</td>
<td>15</td>
<td>3</td>
<td>37</td>
<td>audit and tax services and education services</td>
</tr>
<tr>
<td>6</td>
<td>Bennett Thrasher LLP3</td>
<td>3625 Cumberland Blvd. #1100</td>
<td>Atlanta, GA 30339</td>
<td>770-306-2500</td>
<td>56%</td>
<td>184</td>
<td>95</td>
<td>31</td>
<td>212</td>
<td>assurance, tax, dispute resolution/forensic auditing, client accounting services, personal financial planning, international tax services, international</td>
</tr>
<tr>
<td>7</td>
<td>EY</td>
<td>55 Ivan Allen Jr. Blvd., #210</td>
<td>Atlanta, GA 30308</td>
<td>404-674-6300</td>
<td>49%</td>
<td>1,568</td>
<td>394</td>
<td>149</td>
<td>2,176</td>
<td>assurance, tax, transaction and advisory services</td>
</tr>
<tr>
<td>8</td>
<td>Greenlight Tax Group LLC dba H&amp;R Block Business Services</td>
<td>340 Atlantic Blvd. #13</td>
<td>Duluth, GA 30096</td>
<td>770-921-2200</td>
<td>48%</td>
<td>46</td>
<td>6</td>
<td>3</td>
<td>46</td>
<td>corporate tax, payroll services, individual tax, state and local compliance</td>
</tr>
<tr>
<td>9</td>
<td>Frazier &amp; Deeter LLC</td>
<td>1230 Peachtree St. NE #1100</td>
<td>Atlanta, GA 30309</td>
<td>404-275-7500</td>
<td>48%</td>
<td>218</td>
<td>102</td>
<td>31</td>
<td>243</td>
<td>audit, tax, employee benefit consulting, process/review/governance consulting, forensic accounting</td>
</tr>
<tr>
<td>10</td>
<td>PwC</td>
<td>105 Peachtree St. NE #1100</td>
<td>Atlanta, GA 30309</td>
<td>404-415-1000</td>
<td>42%</td>
<td>1,427</td>
<td>486</td>
<td>102</td>
<td>1,427</td>
<td>assurance, tax, and advisory services, including business transformations, improving business processes</td>
</tr>
</tbody>
</table>

1 Only firms with 20 or more professionals in Atlanta were considered for this listing.
2 A professional is defined here as one required to have continuing education hours. All figures are current as of February 2015.
3 Company submitted a statement of verification supporting figures.

SOURCES: Atlanta Business Chronicle research and the firms
“I also think as we become more and more virtual, we will need stronger skills in qualifying these partner relationships, monitoring them and quickly managing and responding to issues,” DenDanto said. “Long-term relationships based on continual improvement should prevail, which will require knowing who you are doing business with on a more intimate level.”

While there are definitely inherent risks associated with these interdependencies, there are opportunities and advantages, Fields said. “If I outsource my data to a provider who’s going to store that data, suddenly I’ve bought in to all the risks that are inherent in that company,” he said. “I’ve now accepted those risks as well. But there’s the flip side. Field added. “All the strategic advantages they have, whether it’s lower cost, faster speed, backup and redundancy, I get that all,” he said. “So there are risks to my supply chain going global or putting manufacturing off shore or having outsourcing my data to another group but there are also opportunities. They might be better, they might be cheaper, they may actually have a better control environment than I would put in myself.”

And the truth is, most companies would not function well without interdependencies on other companies, Fields said. “They save a lot of money. They get a competitive advantage. They’re actually good things,” Fields said. “All you want to do is make sure your company and your people are aware of the interdependencies and that you’re thinking about them.”

That’s where a good company auditor can come in handy, according to Fields. “It’s important to note that there are two sides to interdependencies—advantages and disadvantages,” he said. “There are risks that companies need to think about and manage. Auditors are really good at pointing out and looking at the risks and the opportunities.”
The 10th Annual Atlanta Conference (TAC)
September 18, 2015
The Cobb Galleria
8 CPEs

Registration is open.
Please contact registrar@theatlantaconference.net for more information.

TAC 2015 Keynote Speakers:

Larry Harrington, CIA, QIAL, CRMA, CAE Raytheon and IIA Chairman of the Board of the 180,000 member Global IIA (Opening Keynote Speaker)

Bill Mulcahy, CIA, CPA, CEO of Mulcahy Consulting (Expert Panel Moderator)

Hala Moddelmog, President and CEO of Metro Atlanta Chamber of Commerce (Lunch Keynote Speaker)

Dan Thurmon, Motivational Speaker and Work/Life Balance Expert (Closing Keynote Speaker)

General Session Expert Panel Members

Susan Bell, EY Atlanta Office Managing Partner

Lynn Clarke, MetroKitchen, CEO

Eric McCarthey, Chair of NACD Atlanta

Paul Lapides, Kennesaw State University

Off Balance on Purpose

Dan Thurmon, Keynote Speaker, Author and Peak Performance Coach

How do you succeed in today’s challenging, changing business climate? How do you sustain the commitment to grow personally and professionally?

Transitions of all kinds can be demanding and difficult. But these moments are also gigantic opportunities to redesign your approach to life and business. As we expand our global reach, this session will give you the encouragement and tools to take action!

In this energizing and “must see” session, Dan Thurmon, author of Off Balance On Purpose, will show you how to take charge of your circumstances, stretch your abilities, and create your blueprint for professional success! Afterward, you will be equipped to:

Own Your Reality, Seek Your Purpose, Lean Forward, Leverage Your Resources, Follow Through

In signature fashion, Thurmon punctuates his message with dynamic demonstrations, incorporating acrobatics, breathtaking stunts, and audience interaction to create a one-of-a-kind experience you will never forget.