In This Issue...

1. President’s March Message

2. February 2019 Conference Recap
   “Fraud Conference”

3. Long Island Chapter’s Upcoming March Conference:
   “Annual IT Conference”

4. IIA Chapter of Excellence Program

5. CNY IIA Seminar

6. IIA Training Opportunities

7. Fraud Alert:
   “A Ticking Time Bomb?”

8. LI Chapter 2018 – 2019 Officers and Board of Governors

Upcoming Events

<table>
<thead>
<tr>
<th>Annual IT Conference</th>
<th>Annual Conference</th>
</tr>
</thead>
<tbody>
<tr>
<td>March, 2019</td>
<td>April, 2019</td>
</tr>
<tr>
<td>Melville Marriott</td>
<td>Melville Marriott</td>
</tr>
</tbody>
</table>
We had a fantastic turnout for our Fraud Conference last month with over 200 attendees! Our conference included a great slate of speakers including a presentation from Nassau County Comptroller Jack Schnirman on the current state of finances in Nassau County and from Yael Fuchs from the NY Charities Bureau who spoke about fraud in non-profits. We also had an informative update on ACFE Report to the Nation on Fraud by Ernest Smith. Our afternoon was a captivating session from Nathan Mueller who told us his story on how he embezzled 8.5 million dollars from ING. There were many lessons learned from his experiences both from a professional and personal perspective. A big thank you to Ernest Patrick Smith our board member and conference chair who put together a fantastic Fraud Conference this year.

As technology continues to advance, we as internal auditors need to stay at the forefront of addressing these risks. The IIA’s Internal Auditor Magazine has a great article this month on internal audit’s role in Cybersecurity. The article talks about internal auditors stepping out of their comfort zone and building their expertise. Internal Audit can add value to your organizations by helping management strengthen controls related to Cybersecurity. This ties right into our upcoming IT Conference which includes a session on Internal Audit’s critical role in Cybersecurity. The conference will also include other hot topics in IT such as top technology trends, data governance and reliability and SOC for Cybersecurity. Our IT Conference is on March 29th and registration is now open for this conference and our brochure for this program is included within this newsletter.

Our annual conference is coming together nicely and will include an Economic Update by John Rizzo from the Long Island Association. We are also going to have a presentation on Auditing Culture as well as a presentation on some hot topics in Human Resources. Our key note speaker will be Justin Jones-Fosu who is full-time husband and daddy who also happens to be an international speaker, an award-winning entrepreneur and author who also presented at the IIA Leadership Conference last year. Justin is an engaging and inspirational presenter and will challenge you to identify with your “why” and live it out now in order to achieve meaningful success. It is sure to be a great presentation. We will also be holding a social in the Library downstairs at the Marriott immediately following this conference. I hope to see you all there.

I also want to let our membership know that we are changing event management system. This is the system that sends out our registration links, surveys & CPE certificates. I ask that you please be patient during this conversion.

As a reminder, all of our programs are held on Fridays at the Marriott located in Melville, New York. We look forward to seeing you all at these upcoming conferences. Should you have any questions, please do not hesitate to reach me at (631) 756-9500 or email me at lagunzo@nsllpca.com.

Kind regards,

Lauren M. Agunzo, CPA
February Conference Recap

We had a fantastic turnout for our Fraud Conference last month with over 200 attendees! Our Annual Fraud Conference was very well attended and was kicked off with Nassau County Comptroller Jack Schnirman who spoke about his top priorities for Nassau County which included modernizing county finances to by implementing technology to track finances in real time and make things more efficient and transparent as well as smart audits which have uncovered more than 16.5 million dollars’ worth of wasteful government practices.

Our next session was presented by Yael Fuchs from the NYS Charities Bureau who presented on Fraud in Not-for-profits. Her presentation talked about protecting charitable assets, protecting donor intent and supporting the work of board members, employees and volunteers. We also had a session on the ACFE Report on Fraud to the Nation by Ernest Patrick Smith and Dimitris Bantileskas. It was an interactive presentation where the audience participated in various fraud polls and we learned about fraud right here on Long Island.

Our afternoon session was presented by Nathan Mueller, a real-life fraudster who embezzled $8.5 Million dollars from ING. Nathan spent the whole afternoon with us highlighting his crime and presented us with all of the fascinating details. He presented the who, what, where when & why and stayed to answer all of our very curious questions. It was truly a fascinating presentation from a reformed white-collar criminal.
2019 Annual Information Technology Audit Conference

Friday, March 29, 2019 – Melville Marriott
8:30 am – 5:00 pm
(8 CPE/CPD Credits)

Event Summary

- Feeling overwhelmed with all the new technology developments during the year?
- Do you increasingly wonder how you will remain relevant in an environment that increasingly relies on automation and analytics?
- Can you adequately respond to stakeholder concerns relating to cybersecurity-related media reports?

If you answered yes to just one of the above questions, the chapter’s annual Information Technology (“IT”) Audit Conference is for you. This year’s conference will be held on Friday March 29 at the Melville Marriott. Our speakers will not only provide guidance in addressing today’s most pressing issues, but will guide you in identifying the skills you will need to remain and become a value added member of your organization in the years ahead.

8:30 AM – 8:45 AM: Chapter Announcements & Introduction to the Conference: Lauren Agunzo, Chapter President & Joel Lanz, Conference Chair
8:50 AM – 9:50 AM: NextGen Internal Audit: David Lehmann, Managing Director, Protiviti

As the pace of innovation continues to accelerate, the Internal Audit profession faces a growing challenge of adapting to change while delivering on it’s core mission of protecting organizational value by providing risk-based and objective assurance, advice, and insight. In response to these challenges leading internal audit functions are pursuing transformation opportunities with the objective of establishing the Next Generation of Internal Audit – an internal audit function that reexamines the foundational elements of the internal audit function; governance, methodology, and technology with a goal of providing more effective assurance and valuable insights to the business through more efficient and technology enabled processes.

David Lehmann is a Managing Director in Protiviti’s New York office focusing on Internal Audit and Technology Risk services, and is responsible for leading Protiviti’s Northeast IT Audit practice. David’s client engagement work includes delivering Internal Audit co-sourcing, IT audit, SOX compliance, IT governance, cybersecurity, and risk management services. David earned a Bachelor of Science degree in Accounting from Binghamton University. He is a Certified Public Accountant (CPA) in New York State, a member of the Information Systems Audit and Control Association (ISACA), the New York State Society of CPAs (NYSSCPA), and Institute of Internal Auditors (IIA). He previously served on local chapter boards for both ISACA and the IIA in New York and Connecticut. David is a frequent speaker at industry events and roundtables on topics such as technology risk assessment, cybersecurity, “next gen” internal audit, cloud computing, and auditing emerging technology risks.


As with any hot topic, there’s a lot of buzz around how analytics and data science will change our professional and personal lives. This presentation is meant to cut through the hype, and give you a practical understanding of these advanced approaches by walking through actual case studies.

Fred Gibbons is a senior manager in the Analytics practice of Deloitte Transactions and Business Analytics LLP with over 13 years of experience leading analytics engagements spanning a variety of focus areas, including: risk management, compliance monitoring, corporate investigations and disputes, and performance improvement.

Philip Matthews is a manager in the Analytics practice within the Deloitte Transactions and Business Analytics LLP with over 8 years of experience for various dispute and litigation engagements including forensic accounting and financial investigations, trading data analysis, FCPA investigations, bankruptcy cases and fraud analysis.

10:55 AM – 11:10 AM: Break
11:10 AM – 12:10 PM: Change Management/SDLC/Agile: Vincent Calabrese, Managing Director KPMG

Vincent Calabrese will describe the evolution of Change Management (CM) and System Development Life Cycle (SDLC) and why effective processes continues to be important. He will walk through risks in each process and control considerations for traditional, Agile, DevOps and SaaS based environments.

**Vincent Calabrese** is a Managing Director in KPMG’s Technology Risk practice. He has 14 years of experience performing both Internal and External IT audits, for large multinational public clients. He has spent his career understanding diverse business operations focusing on IT and SAP, while assessing risks, and then evaluating, designing or implementing processes and controls to mitigate risks. Vincent is a certified SAP Business Solution Consultant and specializes in SAP ECC, GRC, BW, BPC and HANA pre/post implementation assessments, Sarbanes-Oxley 404, General IT Controls, SOX implementations, GRC/SOD assessments and various business processes including RtR, PtP and OtC.

12:10 PM – 1:10 PM: Lunch

1:15 PM – 2:15 PM: Data Governance and Reliability: Michael Fiore, Senior Director Accume Partners

Michael Fiore will be speaking to us on the following topics surrounding Data Governance, its definition, importance and impact in the current market conditions. The Regulatory focus on Data Governance the responsibilities of companies on how they are required to manage their data. Key Risks around Data Governance. Specifically, around the Structure, Inventory and Quality issues surrounding data governance risks. And last but not the last the Data Protection Cycle and the maturity model of companies managing their key data.

**Speaker**

**Michael Fiore** is a Senior Director with Accume Partners based in New York. He has 21 years of audit experience in IT Audit & Security with demonstrated skills in Information Technology, Network Security Vulnerability Assessments, Cyber Security Risk Assessments, NYS DFS 500, Regulatory & Compliance, Higher Education and Financial Services industries. Prior to Accume, Michael was the Managing Director, Information Technology Audit & Compliance Services Practice Leader with CBIZ Risk & Advisory Services, serving as the industry leader for Financial Services, Insurance, Real Estate Investment Trusts, Public Sector/Government, Professional Services, and Technology industries.

2:15 PM – 3:15 PM: SOC for Cybersecurity: John Hoffman, Partner Nawrocki Smith LLP

An overview of the AICPA’s cybersecurity risk management reporting framework. The learning objectives will include an understanding the reporting framework, why it is important, who will benefit from the reporting and how organizations’ can use it as a common platform to describe, evaluate and monitor their cybersecurity risks.
**John Hoffman**, CPA/CFF/CITP is a partner of Nawrocki Smith LLP specializing in forensic accounting and dispute resolution services. Mr. Hoffman earned a BBA in accounting from Hofstra University. He is a Certified Public Accountant (CPA), Certified in Financial Forensics (CFF) and Certified Information Technology Professional (CITP). He is responsible for providing insurance claim consulting services, business valuation, fraud examinations/forensic accounting and dispute resolutions services. On numerous occasions he has been qualified as an expert witness in both federal and state courts. Examples of his services include; examinations of accounting policies and internal controls (SOC Examinations), loss earnings/lost profits analysis related to insurance claims, economic damage calculations, healthcare consulting services, business valuations and fraud investigations.

**3:15 PM – 3:30 PM: Break**

**3:30 PM – 4:45 PM: Internal Audit’s Critical Role in Cybersecurity: Russel Safirstein Anchin**

**Digital Risk Solutions and John Curran Redpoint Cybersecurity**

Internal audit has a critical role in helping organizations in the ongoing battle of managing cyber threats, both by providing an independent assessment of existing and needed controls, and helping the audit committee and board understand and address the diverse risks of the digital world. This session will give some real world examples of cybersecurity breaches, how they were handled and what internal auditors should be doing to help their companies prepare for the inevitable.

**Speakers**

**Russell Safirstein** is Partner in Charge of Anchin Digital Risk Solutions LLC (ADRS), a subsidiary of Anchin Block & Anchin that delivers and develops technology-driven risk and compliance advisory, and analytics-based services. Prior to joining Anchin, Russell was a Partner with Prager Metis Technology, leading their AI and Machine Learning initiatives, in addition to their cybersecurity and risk advisory practices. He also co-founded Paracon Group, and led its advanced analytic delivery platform as well as the balance of its risk advisory services. He was the General Auditor for Liquidnet, where he started the Internal Audit function of this growing organization. As the Deputy General Auditor for MetLife, he was able to transform the internal audit function through technology and business process improvements. For nearly ten years, Russell was SVP and Chief Auditor for Roslyn Savings Bank. Russell received his B.B.A in accounting from Adelphi University.
John Curran is CEO and Co-CISO for Redpoint Cybersecurity, a team of 35+ credentialed ethical hackers and security consultants, which he founded in partnership with Anchin, Block & Anchin in 2017. Prior to starting Redpoint John was Director of Commercial Cybersecurity for a DC-area IT Services and Cybersecurity firm with more than 500 engineers, where he ran both commercial and U.S. government projects and managed a specialized practice that included ethical hacking and incident response services. His executive leadership experience spans more than 15 years in total. He holds a JD and an MBA/MS, in addition to a number of advanced technical certifications, including Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Web Application Penetration Tester (GWAPT), Certified Mobile Applications Security Analyst (GMOB), and Certified Incident Handler (GCIH).

4:45 PM – 5:00 PM: Conference Summary and Conclusion, Joel Lanz Conference Chair
IIA Upcoming Chapter Conference

Friday, March 29, 2019
Full-Day Program

Check-in and breakfast begin at 8:00 a.m. Program begins at 8:30 a.m.
Lunch will be served at approximately 12:15 p.m. Dress is business casual.

How to Register:
Please use the following online registration link: http://www.cvent.com/d/p6qw28/4W

If you are having trouble with the link, notify Carolyn Leahy at Carolyn.Leahy@nationalgrid.com. Cancellations must be made at least 24 hours prior to the event by contacting Lauren Agunzo at lagunzo@nsllpcpa.com.

For Making Payments Offline:
You should register online (see above) and in the payment section, select “check” or “other.” If not registering online, please contact us at LIIA@nsllpcpa.com or call Lauren Agunzo at (631) 756-9500 x 229 at least 24 hours before to reserve your seat. Then complete and enclose this registration form, along with your check payable to the IIA Long Island Chapter, and mail to: Institute of Internal Auditors LI, P.O. Box 442, Smithtown, New York 11787 or bring it the day of the seminar.

<table>
<thead>
<tr>
<th>Name(s)</th>
<th>IIA Member $175 Each</th>
<th>Non Member $200 Each</th>
<th>Student $30 Each</th>
<th>No. of Prepaid Subscriptions Applied</th>
<th>CPE Y/N</th>
<th>CPD Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>$</td>
<td>$</td>
<td></td>
<td>#</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Company Name: ____________________________________________
Address: ____________________________________________
Phone Number: ____________________________________________
E-Mail Address: ____________________________________________

Volume 24 March 2019  Issue 6
Directions to the Melville Marriott:

**From New York City:** Take the Long Island Expressway (Route 495) to Exit 49 South. Take the ramp (right) onto the South Service Road. Turn left (North) onto Old Walt Whitman Road (Walt Whitman Road).

**From Eastern LI:** Take the Long Island Expressway (Route 495) to Exit 49 North. Take the ramp (right) onto the North Service Road. Turn right (North) onto Old Walt Whitman Road (Walt Whitman Road).

In case of weather emergency, the Melville Marriott phone number is (631) 423-1600.
Chapters of Excellence

PURPOSE
The IIA’s Chapter of Excellence program was developed to recognize chapters for their belief in quality education and support of the Certified Internal Auditor® (CIA®) designation, specifically through The IIA’s CIA Learning System® program. The program provides access to high-quality CIA exam preparation resources and helps members achieve their CIA certification goals.

WAYS TO QUALIFY

OPTION 1: Offer a live or online IIA CIA Learning System exam prep course within your chapter area. This may be a course sponsored by your chapter or in partnership with an IIA-approved college/university partner in your chapter area. Chapters may also qualify by co-sponsoring courses with another chapter. A minimum of 2 course parts must be offered each calendar year.

OPTION 2: Promote a live or online IIA CIA Learning System exam prep course occurring outside of your chapter area. This may be a course offered by IIA Global, an IIA Conference/Seminar, another IIA Chapter, or an IIA-approved college/university partnership outside of your chapter area. A minimum of 4 course parts must be promoted each calendar year. A list of qualifying courses may be found at www.learncia.com/classes-offered.

CHAPTER BENEFITS

• Exclusive VIP reception for chapter leaders attending The IIA’s Leadership Academy.
• Recognition at Leadership Academy.
• Chapter of Excellence lapel pin for chapter leaders attending Leadership Academy.
• Chapter of Excellence recognition tile ad to place on your chapter’s website.
• Chapter of Excellence certificate.
• 75 CAP points awarded under “Professionalism” (Tier 2) if 75% of task requirements are met in the CIA Learning category.

REQUIREMENTS TO QUALIFY

• E-mail announcement to your chapter members to promote the course.
• Postcourse dates and information on your chapter’s website.
• Place an announcement in your chapter newsletter.
• Announce the course at a chapter event.
• Exclusively post The IIA’s CIA Learning System tile ad on your chapter website’s homepage and link to www.learncia.com.

IMPORTANT DETAILS

• Instructor materials and discounted student materials are available for chapters who wish to offer a course. Please contact Kelly Quinn at kelly.quinn@theiia.org for more information.
• Chapters may offer or promote a live or online course.
• Chapters must complete the electronic tracking form by March 1 each year to qualify.
• Requirements must be completed 4 weeks prior to course date and date of completion must be documented on the electronic tracking form.
• If your chapter does not have a newsletter or a chapter event occurring, to qualify you must execute an electronic announcement to your members and post the information on your chapter’s website.
• Qualifying chapters will be announced each year at The IIA’s Leadership Academy.

Get complete details at www.learnCIA.com/ChapterOfExcellence.
CNY IIA Three Day Seminar (24 CPEs)
Presented by MIS Training Institute
Successful Audit Data Analytics
April 29 – May 1, 2019
Embassy Suites at Destiny USA, Syracuse, NY

Looking for an MIS training course for a fraction of the cost, at a new 4 star venue and with lower travel costs?

If so, consider this seminar.

Date: April 29-May 1, 2019/ Monday through Wednesday
Time: 8:30am to 4:30pm
CPE: 24 CPE credit hours
Cost: $725 IIA members
$825 non-members
(includes continental breakfast and lunch)
Venue: Embassy Suites at Destiny USA Syracuse, NY
Embassy Suites is just steps from the 6th largest mall in the U.S., providing all kinds of dining and entertainment options for after the training sessions. This brand new hotel features all of the signature amenities offered at Embassy Suites. A limited number of rooms are being held at a reduced rate of $149, until March 31st. This rate includes free made-to-order breakfasts featuring omelets, potatoes, bacon, fruit, pastries and more. Also included are evening receptions featuring complimentary drinks and snacks.

Course Description: Hands On
In this three-day seminar attendees will learn everything they need to effectively integrate data analytics, or CAATs (Computer Assisted Audit Techniques), into an audit process. You will learn how technology can be used to more efficiently and effectively achieve desired results and brainstorm analytics across most major business cycles. You will learn how to progress from basic analytics into a fully automated/repetitive mode, and learn the basics of Continuous Auditing. We will review common hurdles and hear how the most successful organizations in the world have been able to exploit the power of data analysis to achieve visible and sustainable value.
This seminar provides critical experience and content for the audit analytics practitioner. You will get a chance to see how to align your analytics with your department’s vision for the use of data analysis. You will get the opportunity to work on real-world scenarios with sample data files, and practice designing effective tests and critiquing and QAing the work of others.
This is a hands-on course that will be providing data analysis examples using MS Excel. You will need version 2010 at a minimum, versions 2013 or higher are highly preferred. Each attendee needs to bring a laptop in order to get the full value from this course. As the course progresses, you will move quickly from understanding basic analytic techniques such as stratifications, summarizations, and duplicate identification into more advanced techniques such as fuzzy matching, Benford’s Law, and statistical and regression analysis. You will explore cutting-edge topics such as visual analytics, risk score carding, and spatial analysis. Regardless of the tool you currently use or plan to use in your department - whether generic like MS Excel or MS Access, audit-centric like ACL or IDEA, or more IT-oriented like SQL or SAS - the standard pseudo-code used throughout the course will allow you to easily take what you have learned and quickly code it in your tool of choice.

About the Instructor…. 

**Jim Tarantino, CISA, CRISC, ACDA**

Jim Tarantino is a Senior Instructor for MIS Training Institute as well as a Manager at RSM, one of the largest accounting and consulting firms in the world. He has over 20 years of information technology, analytics, audit and GRC experience with a recognized expertise in developing solutions to enable data-driven auditing, risk assessment and investigations. Prior to joining RSM, he was the Client Solutions Director for High Water Advisors, a consulting firm specialized in using technology to help organizations improve governance, risk management, compliance (GRC) and audit processes. He has also held a number of GRC practitioner roles including Solution Lead/Practice Manager for ACL Services, Senior Auditor at RTI International, and various management positions at Nortel Networks implementing an HR analytics program. Mr. Tarantino holds a bachelor’s degree in Psychology and master’s degree in Industrial/Organizational Psychology from North Carolina State University. As a member of the IIA, ISACA and ACFE, he participates in local chapter activities, including serving as an instructor for CISA certification exam preparation.

**Registration information**

http://www.eiseverywhere.com/387742

Registration deadline is April 1, 2019. Seating is limited, so please register early to reserve your seat.

Cancellations after April 1, 2019 will be non-refundable. Substitutions can be requested at any time up until the time of the seminar.

Link for hotel registration at discount rate:
http://group.embassysuites.com/cnyiia

Any questions, contact Lynn Wilber
lwilber@cfglife.com or call 315-471-5656 x7498.
More Seminar information
Learning Level: Intermediate
Advanced Preparation: None
Field: Auditing
Delivery Method: Group-Live

Who Should Attend:
Internal and External Auditors; IT Auditors; QA personnel; IT Security Managers; Consultants

Seminar Agenda
1. Integrating Data Analytics Across the Audit Process
   • stages of the data analysis process
   • enabling the various stages for data analysis with technology
   • applying data analytics to risk assessment, audit planning, fieldwork and testing, reporting, and follow-up and monitoring

2. Pros and Cons of Common Data Analysis Tools
   • MS Office: MS Excel, MS Access
   • Excel add-ins: PowerBI, TeamMate Analytics, ActiveData
   • audit-centric client/server: ACL, Arbutus, IDEA, InfoZoom
   • statistically-based: IBM Analytics, SAS, Minitab, R
   • IT-centric: SQL, Alteryx, Lavastorm
   • business intelligence: Cognos, Business-Objects, PowerBI
   • specialized: SAP
   • dashboarding: Tableau, Qlikview, Spotfire, Lumira

3. Analytic Development Cycle
   • design strategy and approach
   • analytic planning and design
   • data access and validation
   • coding/development
   • testing/quality assurance (QA)
   • script implementation and optimization
   • process differences for ad-hoc vs. continuous testing

4. Planning Data Analytics Projects
   • brainstorming analytics ideas
   • evaluating analytic level of effort and ROI
   • prioritizing data analytics for use in audits
   • making effective data analytic requests

5. Planning for Data Access
   • mapping key systems
   • understanding various data access technologies and techniques
   • understanding various data formats and file types
   • effective negotiation with IT
   • data verification procedures
   • data security and retention

6. Advanced Analytic Design Techniques
   • complex string comparisons and fuzzy matching techniques
• address comparisons
• trending and time series
• Benford’s analysis
• smarter sampling techniques
• statistical and regression analysis

7. **Working with Standard Data**
   • national ID numbers
   • vendor identification numbers
   • postal codes and address abbreviations
   • area codes
   • credit card numbers

8. **Leveraging External Data Sources**
   • watchlists
   • surveys and benchmarks
   • geocoding and address standards
   • ISO codes
   • industry codes
   • social media & web content

9. **Reporting and Interpreting Results**
   • documenting analytics in the audit working papers
   • presenting results in a meaningful way
   • overlapping results
   • analytic precision

10. **Developing Appropriate Standards**
    • naming conventions and scripting guidelines
    • code documentation
    • requirements definition
    • data verification, QA and testing
    • security and archiving

11. **Making Analytics Repetitive and Continuous**
    • scripting and automation
    • design considerations
    • changes to data extraction and analytic logic

12. **Advanced Topics and the Evolution of Analytics**
    • continuous monitoring
    • dashboard and visual analytics
    • score carding
    • predictive analytics
    • spatial relationships and mapping

13. **Common Analyses in Major Business Processes**
    • Record-to-Report (R2R)
    • Purchase-to-Pay (P2P)
    • Forecast-to-Stock (F2S)
    • Order-to-Cash (O2C)
    • Hire-to-Retire (H2R)
    • Process-to-Application (P2A)
Tuesday, March 26 – Thursday, March 28, 2019

The Public Sector Audit Center is hosting its Virtual Symposium, Preparing Public Sector Auditors for Today’s Terrain, on Tuesday, March 26 and Thursday, March 28 from 1:00-3:00 p.m. ET each day. This premier online training opportunity provides government auditors a chance to learn and engage through a convenient and flexible web-based console. Join us for a dynamic four-part symposium specifically designed for the public sector auditor. Attendees will learn how to manage political pressure, build effective cross-department management, use new techniques to investigate fraud, and identify emerging and atypical risks.

Join us in Sunny, Southern California
The IIA’s 2019 International Conference will be held 7-10 July in Anaheim, CA. When you think of Southern California, you envision a locale like no other, equally rich and relaxed, sunny and subdued, educational and entertaining - a place with... A Vibe All Its Own.

Internal auditors from all over the globe will converge on Southern California to gain new perspectives, insights, and best practices relevant to all levels and industries.

With a theme of "A Vibe All Its Own," the 2019 IIA International Conference will deliver a program that delves into timely issues impacting the profession. On top of earning CPEs, you will have the opportunity to network with fellow auditors from other countries, share ideas, challenges and solutions, and hear from global leaders on topics that apply across the board.

If you have any questions regarding accommodations, visas or the event please contact IC2019@executivevents.com.

The IIA requires holders of its certifications and qualifications to report CPE or CPD credits by Dec. 31. For those who have yet to earn their required credits, including two in Ethics, opportunities remain to do so with IIA Training, from in-person seminars, online and OnDemand courses, and webinars, to Internal Auditor quizzes.

Review requirements and report your CPE/CPD credits now.

Prefer In-Person Trainings?

For a list of upcoming in-person trainings in New York City Please Click the Link Below

Training Opportunities at the Microtek Training Facility in New York City
"Rat" and "snitch" are among the terms Thesaurus.com offers as synonyms for "whistleblower." The other 13 are just as negative; not even one is neutral, much less positive. It's the kind of uniform disapproval you'd expect in synonyms for "villain." And these aren't just words in a book; they're manifestations of beliefs that incite and legitimize retaliation for perceived breaches of trust.

So, when someone in a position of authority characterizes whistleblowing as treachery, it unleashes powerful forces that coerce all but the most determined individuals into silence. Blowing the whistle truthfully is no defense when you're marked as a traitor. Those brave enough to speak out sometimes pay for it with their lives.

Witness the fate of Daphne Caruana Galizia, the Maltese investigative journalist assassinated by an unidentified car-bomber. (See Malta Car Bomb Kills Panama Papers Journalist by Juliette Garside, The Guardian, Oct. 16, 2017.) "The situation is desperate," Caruana Galizia wrote on "Running Commentary," her anti-corruption blog, an hour before being blown to bits.

Only four months earlier, Facebook had closed the user account of Malta's national trade union chief for inciting his followers to demand that critics of the government be stoned in public. The same official serves as an advisor to the prime minister's cabinet. For years, whistleblowers in Malta — who had no other way to expose fraud — told Caruana Galizia about foreign and domestic politicians, executives and organized criminals engaging in bribery, tax evasion and money laundering, which she then reported in her blog.

According to a Nov. 25, 2017, article by Tom Kingston in The Times of London, a whistleblowing private banker in Malta had leaked to Caruana Galizia information about a secret Panamanian bank account through which the prime minister received bribes from foreign rulers.

In 2015, 11 million documents, leaked from Panamanian law firm Mossack Fonseca, described 200,000 shell companies the firm formed to hide the wealth of powerful figures from around the world. Among those holding such accounts were Malta's energy minister and the prime minister's chief of staff, both of whom claimed their deposits were legitimate and unrelated to their boss. Nevertheless, the possibility that the various Maltese accounts were illicitly connected was a red flag too bright to leave unexamined. So, Caruana Galizia reported the whistleblower's allegation on her blog, and the prime minister threatened to sue for libel. But before any legal action could materialize, Caruana Galizia was murdered and the whistleblower fled to England, where she told The Times, "If I go back to Malta now, I will not be alive for very long."

Some might consider Malta — a member of the European Union since 2004 — as an outlier in a supranational group widely regarded as the world's most progressive governmental entity. But the
power elite in other EU nations also threaten the press and the whistleblowers it gives voice to. Take, for example, Miloš Zeman, president of the Czech Republic, which along with neighboring Slovakia joined the EU when Malta did. Speaking at a press briefing in Prague four days after Caruana Galizia's murder, he smilingly brandished an imitation assault rifle. On its stock were inscribed the Czech words for "At journalists."

The Post also reported that Zeman had told Russian President Vladimir Putin that there was a "need to liquidate journalists," although he later backtracked his comment after his critics pointed to accusations that the Russian government could be behind reporters' murders. Regardless, such incitements — despite their occasional joking tone — understandably inhibit the press and whistleblowers. That, of course, is their purpose.

Corruption in Central Europe

"People in government here have great power," says Ján Lalka, CFE, founder and managing director of Surveillance, a financial crime investigative agency with offices in Prague, Czech Republic and Bratislava, Slovakia. With 14 years of fraud-fighting experience in the region, Lalka understands corruption there as only a native can. "Everyone sees a lot of dishonesty at the top, but they don't know who'd be better," he says. "In Slovakia, things would improve if we had independent media, police who have permission and the ability to investigate serious fraud, unbiased prosecutors and judges who aren't corrupt — but major scandals indicate that we don't. It strongly discourages whistleblowing."

The EU exerts pressure on member states that violate its Charter of Fundamental Rights, which guarantees dignity, freedom, equality, solidarity, citizens' rights and justice. Unfortunately, the EU has little prosecutorial power over its sovereign nations (See the "Background" section.) And that makes it hard to reduce corruption where the government commits or permits it.

Some nations fare better

Elsewhere, countries with a longer history of democracy encourage whistleblowers to come forward. Businesses that neglect signs of fraud usually pay the price when it comes to light. Excuses generally don't protect them from fines or even prosecution. So, not being hostile to whistleblowers isn't enough; businesses must actively support them. That means giving employees, suppliers and others good reason to believe that trustworthy company officials will maintain whistleblowers' confidentiality, promptly investigate their reports and take action as necessary, including notifying law enforcement where appropriate.

"Transparency and swift response are key elements in an effective whistleblowing program," says Jonathan T. Marks, CFE, CPA, partner and leader of regulatory investigations and compliance practice at Marcum LLP, a global public accounting and advisory services firm with headquarters in New York.

With more than three decades of experience investigating corruption and other fraud, Marks took particular note of the 2015 directive then-U.S. Deputy Attorney General Sally Yates issued to U.S. attorneys on investigating corporate misconduct.
"Known simply as 'the Yates memo,' " Marks says, "it instructed federal attorneys to prosecute individual executives who knew or should have known of wrongdoing but failed to disclose all relevant facts to the government, regardless of whom they implicate."

Yates wrote, "To be eligible for any cooperation credit, corporations must provide to the Department [of Justice] [DOJ] all relevant facts about the individuals involved in corporate misconduct. … Companies cannot pick and choose which facts to disclose. … If a company seeking cooperation credit declines to learn of such facts or to provide the Department with complete factual information about individual wrongdoers, its cooperation will not be considered a mitigating factor pursuant to USAM 9-28.700 et seq."

Also, provisions in the Dodd-Frank Act (pages 5ff) and the Sarbanes-Oxley Act (section 1107) prohibit organizations from retaliating against whistleblowers or employees whose duties relate to whistleblower support. At issue is whether Dodd-Frank applies to persons who've reported fraud other than to the Securities and Exchange Commission (SEC). The court's verdict won't affect whistleblowers who file their complaints directly with the SEC.

"Companies that ignore these laws do so at their peril," Marks says. But many CFEs wonder how they can persuade senior management to carefully share information upon discovery of a major internal fraud. Marks points to the Yates memo. "The SEC will more likely than not come after managers who knew of bad behavior and didn't do everything possible to investigate and end it. You can't fight fraud by hiding it or directing it away from the board and external auditors. Instead of trying to cover up, management should seek more information."

One source stands out, and CFEs should frequently call management's attention to it. Year after year, tips provide the most leads on undetected fraud. So, why do some companies with whistleblower programs still get blindsided by fraud? Because their systems look fine on paper but fail to measure up in actual practice.

"Tips come in many forms — emails, calls to hotlines or customer service, notes under doors, conversations with managers and so on," Marks explains. "More than a few organizations don't formally capture them all. A case management system that doesn't record every allegation and investigation is incomplete. When tips die on the vine deep within a company, it can't fully understand its own fraud profile or deal with it effectively."

Of course, there's no point in amassing historical information if you don't use it. "Companies should continually comb their case management systems for yellow and red flags that, taken collectively, could point to signs of recurring fraud," Marks adds. "And when a whistleblower leaves any kind of identifying information, examine that person's reporting history, if any, without compromising the source's confidentiality. That history might offer clues to the source's credibility."

According to the ACFE's 2016 Report to the Nations, employees (51.5 percent), customers (17.6 percent) and vendors (9.9 percent) were the biggest groups among identified sources of tips. Information of this nature helps companies ensure their whistleblowing programs meet the needs
not only of employees, but also of customers, vendors and others who might provide valuable anti-fraud intelligence.

Operational competence alone won't carry the day, though; strong stewardship is also essential. "Some managers think setting up a whistleblower program is a finite task," says Sean McAuley, CFE, senior fraud manager at Anderson, Anderson & Brown LLP (AAB), a global chartered accountancy and professional services firm headquartered in Aberdeen, Scotland, capital of the North Sea oil and gas industry. "Absolutely not; it's an ongoing responsibility. You can't just tick the box and say, 'Whistleblower program done!' I'm sorry, but that doesn't work."

McAuley, with 25 years of fraud-fighting experience, leads the AAB team providing external whistleblower support to companies across the globe. "People who report fraud have guts, but they're not stupid or reckless," he says. "A whistleblowing program will never be effective if it doesn't inspire their trust and confidence."

The best way to get it, he adds, is to staff the telephone hotlines and websites with experienced anti-fraud professionals who understand the technical nuances and importance of what whistleblowers have to say and how much they risk by speaking out. It also means the organization immediately acknowledges receipt of their reports, keeps confidential the details they've revealed about their identity, and ensures it will promptly look into the issues they've raised. "CFEs should help organizations get these fundamentals right," McAuley says. "If they don't, their whistleblower programs will fail."

One of the greatest challenges in managing a whistleblower program is prioritizing the tips it receives. "Companies shouldn't let low-priority reports consume resources they ought to devote to critical tips," Marks advises. "Besides delaying the investigation of serious fraud, it exposes them to regulatory censure."

Marks recommends that CFEs advise their clients to classify and prioritize tips into five categories — from the least dangerous threats, level one, to the most dangerous, level five. "This speeds up and improves the organization's response," he adds. "Say a tipster alleges the CFO is manipulating revenue. Many companies' corporate structure is complex, especially if they operate in multiple jurisdictions. You've got to identify sources of relevant information, gather and analyze it, then investigate them. That takes time, sometimes a lot. You might interview some sources a second — even third — time to get the whole truth."

"CFEs also should impress upon their clients the importance of sharing information and seeking the active involvement of groups — for example, HR, internal audit, compliance, legal, IT — within whose purview each allegation of wrongdoing falls," Marks says.

Internal staff can satisfactorily investigate allegations assigned to triage levels one, two and three. But allegations involving legal matters, financial statements or senior managers should be assigned to triage levels four or five because of their potentially catastrophic effect on the organization. Because regulators sometimes question the independence and professional skepticism of internal investigations in such cases, CFEs should strongly recommend engaging outside investigators to perform them.
Sometimes, the discovery of additional information reveals an allegation is more serious than originally thought. "Then raise the triage level and bring in additional groups and skills," Marks says. "And always follow established protocol, no matter what. Your clients must never defer or shut down an investigation before it's complete."

Marks calls CFEs' attention to a current SEC investigation into retaliation against corporate whistleblowers. Former PepsiCo General Counsel Maura Smith told the commission in 2017 that the company fired her in 2012 in retaliation for the way she handled an internal probe into Foreign Corrupt Practices Act violations by a PepsiCo subsidiary in Russia. But PepsiCo said it hadn't engaged in any retaliatory conduct.

Smith left the company after signing a non-disclosure agreement and receiving a $6 million separation package. And, thus, the situation remained ... until 2017, when the SEC began an investigation into whether U.S. corporations were using employment contracts to discourage employees from reporting wrongdoing. As part of that probe, the agency subpoenaed Smith, who then shared the previously untold side of her story.

Marks says that when a successful senior executive suddenly leaves her coveted position to "pursue other opportunities," CFEs should look for red flags that might lie behind that bland assertion. He notes that ACFE Research Director Andi McNeal, CFE, CPA, in an ACFE Insights blog post, "Exit Interviews: An Overlooked Tool in the Anti-Fraud Toolbox," wrote that "[... few organizations] use these interviews as a formal element of their anti-fraud programs, leaving them vulnerable to missing candid and crucial information about ethical issues and blind spots, and even the warning signs of potential or existing fraud." McNeal also identified several key questions to pose during exit interviews.

The Long Island Chapter would like to thank Fraud Magazine for allowing us to reprint this fraud article in our Newsletter.
## Executive Board

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lauren Agunzo</td>
<td>President</td>
</tr>
<tr>
<td>Jeffrey Speed</td>
<td>EVP &amp; Treasurer</td>
</tr>
<tr>
<td>Biju Beegum and Adrian Lawrence</td>
<td>VP &amp; Asst. Treasurer</td>
</tr>
<tr>
<td>Vikas Dutta</td>
<td>VP &amp; Chief Information Officer</td>
</tr>
<tr>
<td>Carolyn Leaby</td>
<td>VP &amp; Asst. Chief Information Officer</td>
</tr>
<tr>
<td>Vincent Colletti and Anthony Cervoni</td>
<td>VP &amp; Operations Officers</td>
</tr>
<tr>
<td>Brian Austin and Larry Karp</td>
<td>VP &amp; Membership</td>
</tr>
<tr>
<td>Thomas Comiskey</td>
<td>VP &amp; Secretary</td>
</tr>
</tbody>
</table>

## Board of Governors

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rocky Shankar</td>
<td>Past President</td>
</tr>
<tr>
<td>Ellen Caravella</td>
<td>Past President</td>
</tr>
<tr>
<td>Lauren Bady</td>
<td>Governor</td>
</tr>
<tr>
<td>Brian Blisard</td>
<td>Governor</td>
</tr>
<tr>
<td>Lucille Brower</td>
<td>Governor</td>
</tr>
<tr>
<td>Roy Garbarino</td>
<td>Governor</td>
</tr>
<tr>
<td>Ed Gelfond</td>
<td>Governor</td>
</tr>
<tr>
<td>Ronald Goldman</td>
<td>Governor</td>
</tr>
<tr>
<td>Pinak Guha</td>
<td>Governor</td>
</tr>
<tr>
<td>Joseph Horowitz</td>
<td>Governor</td>
</tr>
<tr>
<td>Prabhat Kumar</td>
<td>Governor</td>
</tr>
<tr>
<td>Michael Lanning</td>
<td>Governor</td>
</tr>
<tr>
<td>Joel Lanz</td>
<td>Governor</td>
</tr>
<tr>
<td>Robert McNair</td>
<td>Governor</td>
</tr>
<tr>
<td>Maria Michaelson</td>
<td>Governor</td>
</tr>
<tr>
<td>Lauren Nichols</td>
<td>Governor</td>
</tr>
<tr>
<td>Russ Safirstein</td>
<td>Governor</td>
</tr>
<tr>
<td>Dawn Scala</td>
<td>Governor</td>
</tr>
<tr>
<td>Alice Seoylemezian</td>
<td>Governor</td>
</tr>
<tr>
<td>Ernest Patrick Smith</td>
<td>Governor</td>
</tr>
<tr>
<td>Jason Stepnoski</td>
<td>Governor</td>
</tr>
<tr>
<td>Rita Thakkar</td>
<td>Governor</td>
</tr>
<tr>
<td>Chris Wright</td>
<td>Governor</td>
</tr>
</tbody>
</table>

## District Representatives

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raquel Marin-Oquendo</td>
<td>District Representative</td>
</tr>
<tr>
<td>Sarah Saunders</td>
<td>District Advisor</td>
</tr>
</tbody>
</table>

## Committee Chairs

<table>
<thead>
<tr>
<th>Name</th>
<th>Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dawn Scala</td>
<td>Historian</td>
</tr>
<tr>
<td>Chris Cariello</td>
<td>Website Administrator</td>
</tr>
<tr>
<td>Lucille Brower</td>
<td>Certification</td>
</tr>
<tr>
<td>Lauren Nichols &amp; Roy Garbarino</td>
<td>Academic Relations</td>
</tr>
<tr>
<td>Ellen Caravella</td>
<td>Finance</td>
</tr>
<tr>
<td>Jason Stepnoski &amp; Lauren Bady</td>
<td>Communications</td>
</tr>
<tr>
<td>Brian Austin &amp; Larry Karp</td>
<td>Membership Development</td>
</tr>
<tr>
<td>Alice Seoylemezian &amp; Rocky Shankar</td>
<td>Evaluate CVENT</td>
</tr>
<tr>
<td>Maria Michaelson</td>
<td>Program Support</td>
</tr>
<tr>
<td>Rita Thakkar</td>
<td>CAE Roundtable</td>
</tr>
<tr>
<td>Russ Safirstein</td>
<td>Employment</td>
</tr>
</tbody>
</table>