WHAT’S NEXT NOW: NEW IDEAS, SOLUTIONS AND APPROACHES TO A RAPIDLY TRANSFORMING FIELD

ISACA's CACS conferences bring together audit, assurance, compliance, risk, privacy, security, governance and information technology professionals from across finance, technology services, insurance, government, military, telecommunications, healthcare, and other sectors.

More than 1,400 attendees were welcomed to the 2018 North America CACS and EuroCACS conferences: ISACA members, volunteers, speakers, sponsors, exhibitors and staff gathered in Chicago, Illinois, USA, 30 April – 2 May, and in Edinburgh, Scotland, 28 – 30 May.

With more than 150 sessions and topics—ranging from transformative technologies, to IT technology governance, to risk-based approaches to security—attendees engaged with experts, networked with colleagues, and gained valuable education. Special focus on the European Union’s General Data Protection Regulation (GDPR) helped attendees better understand the new regulation.

SPEAKER INSIGHTS

“Auditing IoT” presentation by R.V. Raghu, ISACA Board Director and Director at Versatilist Consulting India Pvt, Ltd: “Do we need to get greedy and collect everything that is possible, or do we only collect the data that makes sense to us? In the post-GDPR world, that is a very important question to ask.”

“Internal Audit Top Considerations for 2018” presentation by Richard Knight, Advisory Managing Director, IT Audit & Assurance, at KPMG: “If using Robotic Process Automation frees up human capital so they can perform different processes, do you still have staff to redeploy if the automation fails?”

“Cyber Resilience for the Changing World” presentation by Leonard Ong, ISACA Board Director and Associate Director at Merck & Co. Inc.: “Live and breathe security by design and privacy by design.”

GDPR Panelist Ken Macdonald, Ph.D., Head of ICO Regions, Information Commissioner's Office: “We will soon be seeing a surge in requests, probably from organizations needing a bit of clarity on the implications of the new act, but also individuals who are starting to enforce their new [privacy] rights.”
OPENING CACS KEYNOTES ENCOURAGE AUDIENCES TO EMBRACE CREATIVITY, UNCERTAINTY

What could a graffiti artist possibly share with information audit and security professionals that would resonate and inspire? Plenty, it turns out. While creating portraits of inspirational icons like the Statue of Liberty and Albert Einstein in real time, opening keynote speaker Erik Wahl reminded North America CACS attendees of when they were also artists. “All children are artists,” he told the hushed audience. “You were an artist until you were discouraged by well-meaning adults.”

After putting down his crayons as a child and embarking on a career in law in which he carefully compartmentalized facts, logic and process, he picked up a paintbrush and found that what he needed to thrive—creativity and risk—it were the missing components in his life. Creative skills aren’t rewarded in rigid corporate and educational structures, Wahl said. By adulthood, these skills have atrophied, which means that you’re less able to navigate ambiguity, complexity and uncertainty.

It isn’t just creating art that can help professionals reopen their abilities to creatively transform their roles and enterprises; Wahl listed traveling, experiencing diversity, networking and learning about challenges other enterprises face as opportunities to help professionals view their roles in a creative lens and see chances for breakthroughs. “It will require stepping outside of ‘business as usual’ and the status quo; you may even be stepping outside of your traditional comfort zones,” he said. The results, however, can be beautiful.

There always will be a level of uncertainty in life, but we should relish that uncertainty, shared EuroCACS opening keynote presenter Caspar Berry. “Imagine a world of no uncertainty...there’s no point to living that life,” he said.

Berry, a renowned poker guru, used his gambling expertise to underscore how embracing risk in a world of uncertainty can lead to rewarding outcomes for technology professionals and their enterprises. While human beings tend to crave safety and security, being risk-averse can stifle opportunity, Berry said. Although enterprises are becoming increasingly sophisticated about leveraging data, it is still rare to have all the information about a given decision that would be ideal. Berry said decision-makers must be prepared to get decisions wrong, as well as to be willing to quickly change course and reallocate resources to adjust to shifting realities.

Berry commented that while everyone is let down by people at times, that is no reason to stop trusting colleagues and friends. “Things can always go wrong...we can’t immunize ourselves from the pain of failure,” he said.

CASPAR BERRY
Screenwriter; speaker on risk, decision making, innovation and leadership; former professional poker player
EuroCACS presentation: “Risk and Decision Making”
@veryloudspeaker

ERIK WAHL
Artist, entrepreneur, best-selling author
North America CACS presentation: “The Spark and the Grind: The Discipline of Creativity”
@ErikWahl
The CACS conferences were held at an interesting time: North America CACS took place shortly before, and EuroCACS immediately after, the 25 May 2018 implementation of the General Data Protection Regulation (GDPR), which impacts all enterprises that do business in the Europe Union (EU) or process the personal data of anyone in the EU.

ISACA Past Board Chair Theresa Grafenstine shared ISACA research in her Leadership Briefs to all CACS attendees; fewer than one in three organizations expected to be fully compliant as of GDPR's implementation date, and only 39 percent said employees had been educated to a satisfactory level about their responsibilities to maintain GDPR compliance.

GDPR also was a major focus of many educational sessions; EuroCACS offered a GDPR Data Analytics & Information Management track, and North America CACS featured a Master Class and several sessions dedicated to GDPR. Industry experts participated in panel discussions at both conferences.

EuroCACS attendees learned from Ken Macdonald, a representative of the Information Commissioner’s Office, which is responsible for implementation and assisting enterprises in complying with the new laws. He noted that regulators will be more apt to look favorably upon organizations that are making a clear effort to comply, even if they have not yet achieved full compliance.

**Some takeaways from both events:**

“Most of what’s going on with GDPR is a governance problem. It’s managing your data to be in line with the company’s or organization’s best interests. The ability and the incentive to reduce your data footprint while increasing your data relevancy, and the importance and the utility of that data, I think is a very positive direction.”
– Andrew Neal  
President, Information Security & Compliance Services  
TransPerfect Legal Solutions

“GDPR is not a checklist, and it isn’t just a legal issue. Data is an enterprise asset, and enterprise means everyone.”
– Theresa Grafenstine  
ISACA Board Chair, 2017-2018

“We will soon be seeing a surge [in requests], probably from organizations needing a bit of clarity on the implications of the new act, but also individuals who are starting to enforce their new [privacy] rights.”
– Ken Macdonald, Ph.D.  
Head of ICO Regions  
Information Commissioner’s Office

“For more information on GDPR, visit www.isaca.org/gdpr
**DIGITAL DISRUPTION: PROACTIVE RISK MANAGEMENT**

In his North America CACS presentation, “Proactive Risk Management and Compliance in a World of Digital Disruption,” Mike Wons drew heavily on his just-completed term as State of Illinois CTO, urging attendees to move tech risk from “conformance to performance” in behaviors and processes, embedded across organizations and the business enterprise.

Wons characterized most risk management as reactionary and not focused on the core. “Security, and risk management, begins at the code level,” he noted.

While some view blockchain as a digital disrupter, Wons, now CTO of SAI Global, sees blockchain as “essential to improving individual security” and proactive risk management.

He said proactive risk management must be continuous, beginning with enterprise visibility to a “risk canvas” that is developed and regularly updated. “We have to think about how to solve things not just for now, but for the future digitalization of the world because that’s just begun. We’re very early on in that,” he added.

**AUDITING THE INTERNET OF THINGS**

ISACA Board Director R.V. Raghu explored “Auditing IoT” in a EuroCACS session, stating that IoT audits should align with enterprise needs and ensure a compliance approach is factored in from the outset. Auditing IoT can help address an array of important questions, including the following:

- How will the device be used from a business perspective, and what business value is expected?
- What threats are anticipated, and how will they be mitigated?
- Who will have access to the device, and how will their identities be established and proven?
- What is the process for updating the device in the event of an attack or vulnerability?
- Who is responsible for monitoring new attacks or vulnerabilities pertaining to the device?
- With whom will the data be shared?

**CONFERENCE POLL: EMERGING TECH**

“What excites you most about the future of technology?”

“Technology changes, innovation and regulations are all changing the financial sector. Now with GDPR, we will see many more players with more solutions. Banks will need to redefine themselves as financial institutions, as well as what they do overall in the market, as competitors and with whom they partner.”

Helga Sigurjónsdóttir
Internal Auditor
Landsbankinn, Iceland

“Technology governance and the governance of innovation is most exciting because businesses and organizations can govern innovation properly. If they do that, they can use technology to transform their businesses and their innovations through change management practices.”

Johnny Johansen
Senior Business & IT Consultant
France

“The rapid changes of technology and the future of technology are most exciting to me and to my team. It’s how we stay employed and valuable to our organization. The challenge of the rapid changes and all the new technology is that people get ahead, implementing it, without considering the compliance and risk that must go along with new technologies.”

Paul Upshaw
Compliance & Risk Manager
Allstate Insurance, USA
ISACA Audit Expert and Past Board Director Allan Boardman’s sage advice for IT audit success, as shared at EuroCACS:

**PERCEPTIONS, POTENTIAL CONFLICTS AND STRATEGIES TO SUCCEED IN IT AUDIT**

<table>
<thead>
<tr>
<th>Potential Perceptions and Conflict Sources for IT Audit</th>
<th>Strategies for IT Audit Success and Trusted Partnerships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tone at the top can drive undesired behavior</td>
<td>Respect business priorities</td>
</tr>
<tr>
<td>Lack of open communication</td>
<td>Establish credibility</td>
</tr>
<tr>
<td>Audit requirements (i.e., things done just because “audit says so”)</td>
<td>Develop relationships at ALL levels: be a trusted but critical partner and advisor</td>
</tr>
<tr>
<td>Check box—things are done just for audit</td>
<td>Get a “seat at the table” early</td>
</tr>
<tr>
<td>(Too) Strict adherence to audit against policies</td>
<td>Be well-prepared and learn from the business</td>
</tr>
<tr>
<td>Pre-audit or clean-up exercises before audits</td>
<td>Be empathetic, reasonable and flexible</td>
</tr>
<tr>
<td>Continuous auditing—being close to the deal flow</td>
<td>Audit findings must be practical and risk-based</td>
</tr>
<tr>
<td>Feelings of being over-audited</td>
<td>Look for opportunities to provide advice and solicit feedback</td>
</tr>
<tr>
<td>Adverse audit points linked directly to pay awards</td>
<td>Communicate, communicate, communicate</td>
</tr>
</tbody>
</table>

**SPEAKING TO YOUR BOARD ABOUT CYBER RISKS**

ISACA 2018-2019 Board Chair Rob Clyde provided guidelines at North America CACS for how to successfully update your board:

1. Give a summary of good and bad news up front (don’t hold the punchline); if you have an ask, tell them at the beginning of your presentation, not the end.
2. Be clear and concise, both in your discussion and in the advance materials for board packet.
3. Be transparent and honest. Don’t give unfounded assurances.
4. If you don’t know something, say so and promise to get back to them.
5. Avoid tech speak and acronyms.
6. Use analogies to aid understanding for non-cyber experts.
7. Articulate business impact, risk, mitigations and plans.
8. Clearly identify anything that requires board action or consideration.
9. Do not surprise your CEO—brief her or him in advance.

And remember: competitive risk may be bigger than cyber risk, so explore new technologies and their potential impact. Avoid becoming a roadblock that slows growth and progress, and enable the safe adoption of new technologies and processes.

**SECURITY LIAISON RESPONSIBILITIES**

This slide is from the North America CACS presentation “How to Build & Grow Your IT Security Team” from Tammy Moskites, Senior Security Executive and Managing Director, Accenture Security:
Between networking breakfasts, panels, half-day seminars and receptions, the SheLeadsTech program offered North America CACS and EuroCACS attendees opportunities to discuss gender parity, the need for mentoring emerging women leaders, and how organizations can make a cultural shift towards inclusivity.

Speakers engaged attendees with stirring stories and authentic anecdotes of policies they shaped and of people who shaped, inspired, and motivated them. They talked of overcoming barriers and bias, challenging conventions and achieving success. It wasn’t only the insights coming from the podiums and panels that resonated so strongly; the ability to connect with other women in tech allowed attendees to find common ground and new allies.

SheLeadsTech Half-Day Seminar “Pearls of Wisdom”

Anne Moises, Scottish government CIO and leader of “Safe, Secure & Prosperous,” Scotland’s cyber resilience strategy launched in 2015 and designed to achieve world leadership and recognition in cyber resilience by 2020, has dedicated her expertise to building and leading the many vectors of Scotland’s cyber resilience program: across public-private enterprise, the educational system, STEM efforts and extensive up-skilling activities. These experiences have reinforced long-held lessons for Moises: collaboration is essential; always build awareness; continue to build skills; and share experiences—the good and the bad.

While Moises described a career path solely in civil service, the career course of Gail Coury, Oracle Cloud global CISO, ISACA Women’s Leadership Council member and SheLeadsTech volunteer leader, has traversed information security leadership roles through her career. Coury balanced her seminar remarks between candid stories of courage and her “pearls of wisdom” list inspired by Oracle’s co-CEO:

- Things need to make sense. Ask questions for explanation and understanding.
- You can recover from a bad decision, but not indecision.
- Just because everything can be put online does not mean it should be.
- Integrity matters; be honest and straightforward.
- If you don’t ask, you won’t get—a lesson she illustrated with her experience in building and winning her case to attend the Stanford executive MBA program, supported by Oracle.
- Don’t stand still—make it happen. Have a sense of urgency.

Quotes from SheLeadsTech Panel on How Diversity Improves or Hinders Risk Management

“Leadership should consider those who are introverted but have more expertise.”
– Shara Evans, Technology Futurist and North America CACS Keynote Speaker

“To find new talent, look in new places. Be authentic and approachable. When I was younger, I had imposter syndrome. Walk across the bridge and tell them they’re welcome. Pull them in; they’ll have loyalty. Put your hand out and make the connection.”
– Theresa Grafenstine, ISACA Board Chair 2017-2018 and managing director, Deloitte & Touche LLP

CONFFEREECE POLL: WOMEN IN TECH

What can individuals do to ensure the future tech workforce includes more women? How about organizations?

“Individuals can mentor junior and high school girls. Organizations should reach out to local schools; my alma mater, Cal State San Bernardino, partners with a Girl Scouts day camp on a cybersecurity business program.”
– Karoline Bednarski, Manager, Platform Assurance IBM Cloud, USA

“Enabling women to move into positions which are more visible in the company that inspires the younger females to move into these positions and to be more valuable. It goes back into not having so much a mentor, but a role model—so, more role models.”
– Hazel Grant, Technology Audit Manager FNZ Group, Scotland

“Girls need to be told that they don’t have to be technical to find their place in this field. It’s a great career for women: it’s a social job that requires organization and analytical skills; you can be the liaison between business and IT.”
– Kelley Smith, Account Executive LogicGate, USA
Today’s technological innovations should create a larger conversation about what leadership should look like in the era of digital transformation, said EuroCACS closing keynote speaker Mike Walsh. Walsh said the deployment of big data and the use of sophisticated algorithms are putting pressure on enterprises to predict customers’ needs like never before.

One of Walsh’s thought-provoking “mind grenades” for the audience: “If you were going to design an AI-first competitor to your business today, what kind of internal and external data would you need to succeed?” Walsh said many organizations already have much of that data on hand and simply need to make better use of it.

From a personnel standpoint, Walsh said organizations need to bring in people who are energized by unknowns and problem-solving. Walsh also encouraged organizations to do a better job of tapping into younger employees and taking their input seriously.

“This is a world being designed for your kids,” said Walsh, who said today’s youth are growing up in “an age of miracles.”

Sharing mind-bending anecdotes about emerging technologies and how they may be used one day, futurist Shara Evans shared her concerns about possible misuse; unrestrained adoption of tech may even change what it means to be human, she believes, when machines and sensors enhance our bodies and our abilities. Having a living body may no longer be relevant if “mind files” become a reality: the ability to download our brains’ knowledge and memories so that we may interact via avatar for generations even after our deaths.

The fallibility of artificial intelligence (AI) needs to be better understood, Evans stated. Changing less than one percent of the pixels in a digital image will fool AI photo recognition; think of the bad actors who will be able to manipulate us with fake videos and images. Misinformation isn’t all that we have to stand against: Evans declared privacy a human right and stated that a privacy violation may be considered a crime against humanity.

“We really need to think ahead to what can happen and balance how we use technologies so that we end up with a wonderful future, rather than a dystopian nightmare,” Evans said. Among the causes for worry, Evans made it clear that the CACS audience would be among those who will protect us from unethical uses of technology. “You will fight the good fight,” she said.
Business demands for IT auditors to be more agile, innovative, strategic and adept with new technology were topics that actively engaged participants in ISACA's IT Audit Leaders Summit at both CACS conferences. ISACA partners, including Deloitte, Protiviti and KPMG, prompted conversation among the business leaders who attended, most from Fortune 500 companies.

At the North America CACS presentation “Internal Audit Innovation—Leveraging Doblin and Agile,” speakers Clay Young and Salman Mohammed, both of Deloitte & Touche LLP, shared data that listed Agile internal audit characteristics that led the captivated attendees to debate how and when Agile principles and processes can be integrated in internal audit, and how to best educate stakeholders on its value in the audit lifestyle.

The value of Agile, attendees described, is that it reduces time, increases value, lets audit teams do more and produces results of value to the business. Young advised, “Pilot first, show the value to management in the face of change and pushback.”

At the IT Audit Leaders Summit hosted at EuroCACS, Rosemary Amato, former managing director, Deloitte Global Finance, EMEA Controller, also triggered significant discussion of Agile auditing in asking attendees for topics of most concern—strategic and tactical—in their jobs. As one attendee said, “There needs to be a change in audit to Agile, given the pace of technology change.”

Emerging technologies—robotics, artificial intelligence, machine learning, quantum computing, blockchain, even mainframe migration—were among the topics listed by IT auditors in the room, as was, not surprisingly, the EU's GDPR. GDPR's compliance date, 25 May 2018, was four days prior to the summit, and this deadline and how each enterprise would meet the challenges of complying were main focuses for attendees.
In his "Using COBIT 5 to Manage Shadow IT" presentation, Professor Christopher Rentrop of HTWG in Germany said that while COBIT 5 calls for a holistic view of IT, the use of shadow IT hinders this integrated view because of its lack of transparency.

Rentrop defined shadow IT as "business process supporting systems implemented and maintained by business departments without being integrated in IT service management." He noted that enterprises’ risk management programs will be unable to deliver on their potential if shadow IT is not properly addressed, given that shadow IT causes organizations’ risk appetite to be exceeded and leads to incomplete risk analysis.

The arrival of the GDPR implementation deadline further underscores the risks of shadow IT since many unknown systems can contain personal data that could lead to compliance trouble.

Similarly, COBIT 5 was named as a solution to governing new technologies such as machine learning, the Internet of Things and big data analytics, as there is increased competitive advantage in the convergence of IT and operational technology (OT), according to Arno Kapteijn, Management Consultant IM/IT at CoCorBan, in his presentation "OT Operating Models Using COBIT 5."

Historically, those areas have seldom been in sync, based on differences in the technologies as well as a cultural divide between IT professionals and OT professionals, who tend to have more of an engineering background.

While full integration of IT and OT into one operating model for technical assets might not be realistic, better alignment can be achieved. To that end, COBIT 5 can serve as a practical framework for the design of an OT governance and management system and can also help make strategic connections between the disciplines.

**EIGHT CRITICAL GOVERNANCE QUESTIONS FOR SECURITY PROFESSIONALS**

From Andrej Volchkov, Consultant at Stramizos:

- Are the board and management involved in strategic information security decisions?
- Who defines the security strategy and policies?
- Who is legally responsible for the security posture and data protection?
- Do you know which business processes are at risk?
- Who owns sensitive data?
- Is your security adapted to meet real business needs?
- Do the business lines participate in security committees making decisions about securing their business processes?
- Do you know if your security expenditures are justified?
- What’s the return on security investment (ROS)?

**HOLISTIC SECURITY: DEVSECOPS**

Most organizations are deploying DevOps to keep pace with the speed of business, and those that are not are likely candidates to go out of business, Robert Stroud, ISACA Board Chair, 2013-2014, ISACA Director, and Chief Product Officer at XebiaLabs, taught at his DevSecOps sessions at both North America CACS and EuroCACS.

Stroud said audit, security and compliance teams should be consistently available to product teams to ensure more agility and improved collaboration at the outset of projects. He also emphasized the importance and value of coding, noting that many organizations deploy code updates on a daily basis now, compared to earlier in his career, when that might have occurred a couple times a year. He said enterprises should look for those with coding skills when making new hires.
SOCIAL MEDIA ROUNDPUP

North America CACS 2018
1,987 posts tagged #NACACS
1.7 million people were reached with 7.8 million impressions

EuroCACS 2018
1,096 posts tagged #EuroCACS
1.2 million people were reached with 7 million impressions

JOIN US NEXT YEAR!


Visit www.isaca.org/conferences to view all ISACA conferences.