Key Takeaways, Quick Lists, and More

Talk about being lean and agile: the global COVID-19 pandemic has forced every industry to quickly rethink its practices and find new solutions. While ISACA had looked forward to welcoming attendees to Baltimore, Maryland, for the North America CACS 2020 conference, 12-14 May, we instead pivoted to an online event. Virtual attendees from 22 countries logged in for education, networking and a bit of fun from their own homes. While a departure from our in-person CACS events, it was amazing to connect and learn together. Enjoy these top takeaways, and we hope to see you next year—in person or online.

QUICK FACTS

- **8** tracks
- **40+** sessions
- **2** keynotes
- **4** workshops
- **800+** attendees
- **11** sponsors
- **6** virtual happy hours

LEGEND

Gain key insights from sessions in the following tracks:

- IT Audit & Assurance
- IT Risk Management
- Emerging Technology and Techniques
- Data Analytics and Information Management
- IT Governance, Compliance and COBIT
- Security/Cybersecurity
- Leadership Development and Career Management
Opening Keynote:

Adventure Athlete Alison Levine

“Fear is okay, but complacency will kill you.”

“Every member of a team is in a leadership position. Leadership is not about title or tenure or how many people report to you. Leadership is recognition that every member of a team has the responsibility to move forward toward a goal.”

“Back up is not the same as backing down.”

“There are two kinds of ego you want on a team:

• Performance ego—people who are good and know they are good. You want LeBron James to be LeBron James.
• Team ego—people who are proud to be part of something that feels collectively more important than anything they could do alone.”

“A lack of failure tolerance stifles progress and innovation and prevents people from taking risks.”

“You don’t have to be the best, fastest or strongest to get to the top. You just have to be relentless about putting one foot in front of the other.”

“You can be scared and brave at the same time.”
Communicating Your Way to a Better Collaboration

From Mary Breslin’s “Difficult Clients and Fixing Problem Relationships” session

- We use a lot of jargon in IT audit. We really can confuse people. Not everyone speaks our language and understands it. **We have to speak to people how they’re used to communicating.**
- You can appeal to people’s pride: they want to run a good department or have good processes.
- Don’t ever tell someone to relax. That won’t go over well.
- Sometimes difficult relationships aren’t repairable, and you have to turn over situations to a colleague. That’s why the work we do is a team sport.

Six Steps to Incorporating Pandemic Risk into a Business Impact Analysis

From Ali Pabrai’s “COVID-19 Cyberattacks Disrupt Business: Opportunity to Transform Cyber Defense Program” session

1. Assess and prioritize essential business functions and processes.
2. Identify the potential impact of a pandemic on the organization’s essential functions or customers.
3. Identify the legal and regulatory requirements for the business.
4. Estimate the maximum downtime associated with the business functions and processes that may occur during a pandemic.
5. Assess cross-training conducted for key business positions and processes.
6. Evaluate the plans of critical service providers for operating during a pandemic.

**Incorporating Pandemic Risk into BIA**

- Assess and prioritize essential business functions and processes.
- Identify the potential impact of a pandemic on essential business functions and processes.
- Identify the legal and regulatory requirements for the business.
- Estimate the maximum downtime associated with the business functions and processes that may occur during a pandemic.
- Assess cross-training conducted for key business positions and processes.
- Evaluate the plans of critical service providers for operating during a pandemic.
  - Financial institutions should evaluate the plans and monitor the services to ensure critical services are available.
  - Financial institutions may wish to have back-up arrangements to mitigate any risk.

**CONFLICT MANAGEMENT**

- An Adversary System
- Win-Win vs Compromise
- Perception, Perspective and Punctuation
- Managing Emotions
- Goals – the many, the multiple and the changing
- Conflict Styles
Why Futurist Guy Herbert Loves Agile

From Guy Herbert’s “Agile, DevOps and Compliance” session

1. Delivers value quickly
2. Focuses on the stakeholder
3. Autonomous team execution
4. Highly adaptable
5. Continuous improvement
6. Predictable cost and delivery
7. Reduces time to market
8. Improves quality
9. Improves productivity
10. Increases employee satisfaction
11. Reduces cost

Leaner, Scrappier, More Efficient

From Prescott Coleman’s “Transforming IA with Lean & Agile Techniques” session

Lean is as exactly as it sounds – it’s about becoming leaner, scrappier, more efficient.

**THREE PILLARS:**

- Energetic collaboration
- Iterative audit execution
- Visual management of audits

“The House of Data is rooted in compliance, risk and policy.”

— Jamie Burgess, from her session with Bob Herman, “Transform Your Data: The Journey to Realize Your RPA and Data Analytic Dreams”
Vendor Risks: Third Party, Fourth Party, and Inviting Your Business Partners to the Party

From Alex Bermudez’s “Getting Granular with Vendor Risks: Adding Business Context & Mapping Data Flows” session

Vendor Risk Challenges are Numerous and Complex

Why vendor risk management?
- New technology, more breaches, greater consequences. We now collect more data on a daily basis than at any other time in human history.
- Current regulations are only the tip of the iceberg.
- Cloud computing is extremely disruptive in the IT space.
- Units like HR, marketing, and IT may have specific requirements for how to get projects done, but those efforts must be coordinated from a privacy and data governance standpoint.

Questions to ask yourself and your organization:
- Do you know your FOURTH-PARTY RISK? Who are the vendors that your vendors do business with, and how will they be held accountable?
- How is the data actually being used? What is its purpose, who is involved and what data transfers are taking place?
- What happens when a business process changes? What new risks could these changes introduce? Be sure to add business context to accurately assess risk.

Manage the process:
- Conduct company-wide awareness training about vendor management risk.
- At an annual vendor review, ensure you are comfortable with their risk posture, ensure scope hasn’t changed and do an analysis if it has.
- Use vendor risk ratings and evaluate specific services for risk.
- Use your legal team to help vet data flows as related to regulatory obligations, or deploy outside counsel on retainer to help interpret specific challenges.
**Mocktails with Megan**

Megan Moritz, director of global volunteer engagement at ISACA, demonstrated her favorite non-alcoholic recipes during a North America CACS happy hour, Mocktails with Megan. You can substitute alcohol into these recipes or enjoy as mocktails.

### Maki’s Margarita

(Megan’s niece calls her Maki)

In a shaker, pour:

- **2 oz** Ritual Zero Proof Tequila Alternative (or substitute any decent gold or silver tequila)
- **1 oz** Agave nectar (or honey if you don’t have the nectar)
- **1 oz** Fresh squeezed lime juice (the juice from one full lime should be about 1 oz)

Add ice and shake for 20 seconds. Pour (with ice) into salt-rimmed glass.

Note: To change things up, throw a couple of slices of fresh jalapeno, a couple chunks of fresh pineapple, or any other fruit you might like into the shaker with the ice and all the other ingredients. The jalapeno/pineapple combo is delicious!

### Wannabe Tom Collins

In a shaker, pour:

- **1 oz** Fresh squeezed lemon juice (the juice from half of a decent-sized lemon should be about 1 oz)
- **1.5 oz** Ritual Zero Proof Gin Alternative (or substitute regular gin)
- **.5 oz** Simple syrup

(To make the syrup, combine equal parts water and granulated sugar in a pan and bring to a boil. Turn off heat and allow to cool. Store in a glass container. A little goes a long way!)

Add ice and shake for 20 seconds. Pour (with ice) into a glass and top with 2 oz of club soda.

### Mexican-ish Mule

In a shaker, pour:

- **2 oz** Ritual Zero Proof Tequila Alternative (or substitute real tequila)
- **.5 oz** Fresh squeezed lime juice (about 1/2 of a lime)
- **.5 oz** Simple syrup

(To make the syrup, combine equal parts water and granulated sugar in a pan and bring to a boil. Turn off heat and allow to cool. Store in a glass container. A little goes a long way!)

Add ice and shake for 20 seconds. Pour (with ice) into glass and top with 3 oz of ginger beer (NOT ginger ale!).

(Megan's niece calls her Maki)
Different Laws, Same Implications: Protecting your Organization

From Victoria Beckman’s “The Current Landscape of Cybersecurity and Privacy Laws” session

A mishmash of laws:

- Each US state has its own laws; there are 54 state laws when you include Puerto Rico, Guam, District of Columbia and Virgin Islands.
- If your company suffers a breach and sells in 14 different states, you must comply with the laws of all 14 states.
- Most of the laws are similar but some have specific requirements (i.e. notifying the state attorney general’s office).
- Two states (California and Oregon) have laws related to IoT devices.
- Some states require an incident response plan; only one state, Massachusetts, requires a WISP – a written information security program.
- Three states (Illinois, Texas and Washington) have biometric privacy laws (Arizona and South Carolina have pending laws).
- Some data incidents may have legal requirements, even if they weren’t a breach or hack (for example, making a file available in a shared server could be considered a data breach in some statutes).

Cyber Risks Call for More Than Internal Personnel

From Kevin Jackson’s “The Virtual CISO: The Future of Cyber Strategy?” session

“Cybersecurity embodies way too much risk to be managed by on-the-job training and to be managed by piecemeal execution.”

Managing cyber strategy is ideal for CISOs: they’re not only strategic but they also manage reporting, metrics, compliance and infrastructure. However, CISO-level talent is rare and expensive. Many smaller organizations must rely on a CIO, director of IT or cyber engineers, which may mean always putting out fires without a strong view into cyber strategy and the risk management needs of cybersecurity.

The virtual CISO, or contract cyber expert/fractional CISO, is like CISO as a service, and the value proposition is enormous. Virtual CISOs often cost less than half of what full-time CISOs do to employ. In this rapidly-evolving threat landscape, even great CISOs can benefit from supplementary virtual CISO support.
Cellular Networks, Fifth Generation: 5G is Coming
From Ferris Adi’s “Securing 5G—Data Risk Management for the Future of Wireless Technology” session

The Impact of 5G on Data Management
• The upgrade to 5G will demand more comprehensive data management and 100% reliability. Organizations must implement and maintain a data management strategy that can not only accommodate larger volumes of data, but also maintain high speeds and eliminate the risk of downtime.
• Preparing for 5G adoption will require reviewing current database capabilities and determining whether existing platforms are sufficient for building and accommodating rapid growth.
• The promise of 5G demands new hybrid cloud data management strategies that allow enterprises to handle larger volumes of data and meet higher standards of reliability and performance.

Metrics Must be Easily Understood by the Board
From Todd Fitzgerald’s “39 Ways to Work with the Board of Directors” session

Cybersecurity metrics assist in:
1 Increase in share value for good governance
2 Increased predictability of business operations
3 Protection from civil or legal liability as a result of absence of due care
4 Critical decisions not based on faulty information
Fast or Slow, Do IT Right
From Mark Thomas’ “COBIT 2019 Spotlight – Governance and Management in a High Velocity Environment” session

Tips & Tricks:
• Remember, you are not the last company in the world to still do waterfall!
• Use both fast and slow IT to ensure proper delivery of services.
• Fast IT methods are NOT immune from governance and compliance.
• COBIT practices and activities are applicable in ALL delivery approaches.
• Consider all governance components, not just process practices.
• Don’t forget to address the silent killer: organizational change and culture.

When he isn’t educating others on all matters of business IT or consulting with global organizations, Mark Thomas enjoys craft beer, as evidenced by his North America CACS Virtual Happy Hour, “The Thomas Takedown,” where attendees sat back, relaxed, and enjoyed a drink while chatting about new and old favorite brews.

Machine Learning is Not Magic
From Andrew Clark’s “Machine Learning Monitoring, Compliance and Governance” session

Machine learning is never going to be used independently of humans, but can help augment humans.

Why machine learning is important:
• New revenue sources; reduces cost
• Accelerates work that used to only be possible by humans; frees up human resources for higher-value work
• More accurate fraud detection
• One of the key technologies in driving economic growth
• Allows us to do things faster/better than we used to
• Revolutionizing existing businesses (Manufacturing, retailing, loan underwriting)

ML is not:
• Magic
• Going to take your job (for majority of professions)
• Always the best tool for the job
Soft Skills for Auditors
From Jason Winters’ and Steve Murdock’s “Navigating Audit Landmines with Soft Skills” session

“People think about auditors as sticking to strict controls. We must continue to stretch ourselves and become innovative in our approaches because they’re rethinking how they operate on a daily basis.”

A Truly Global Network
Attendees from 22 countries logged in for live sessions, happy hours and networking. Hats off to our friends who would usually be asleep but knew they couldn’t miss ISACA’s first virtual conference!

Countries represented:

- Australia
- Austria
- Bahamas
- Brazil
- Canada
- Curaçao
- Dominican Republic
- Ecuador
- Egypt
- Germany
- India
- Israel
- Japan
- Mauritius
- Mexico
- Nigeria
- Switzerland
- Trinidad and Tobago
- United Arab Emirates
- United Kingdom
- United States of America
- Venezuela
Getting Ahead of Fraud
From Mary Breslin’s and Keith Barber’s “Fighting Fraud with Data Analytics and IA” session

Red flags — look for attributes:
• Of the actual fraud or transaction?
• Of the concealment?
• Of the conversion?
• What’s missing?
• Or, how the fraud is managed?

Common areas for fraud analytics:
• Fraudulent disbursements – accounts payable
• Employee expenses
• Payroll
• Inventory & fixed assets
• Financial statements

“No two organizations are at risk in the same way because all organizations are unique.”

“It will always be easier to prevent fraud than to detect it.”

Remember: anomalies in financial information and/or data may occur and may not be representative of fraudulent activity.

Holistically Approaching Privacy
From Ashwin Chaudhary’s “Privacy Assurance: Growing Need for Tools” session

Privacy is not just about managing cookies and opt-ins and opt-outs; it must be a holistic approach with privacy by design, data minimization, tokenization, etc. There are a variety of privacy tools available, including COBIT. Be wary of third-party providers: they often don’t have the proper approach to managing the data lifecycle. You must continuously monitor and audit vendors, or you are likely to have breaches.

Why is there such growing opportunity in privacy assurance?
1 Increasing IoT devices and risks
2 Increasing data size and use of AI
3 Increasing human error in data breaches
4 Increasing social media user data compromised
5 Organizations using mainly legal to manage privacy
6 Lack of a holistic and collaborative approach
7 Increasing compliance mandates
8 Increasing demand
Examples of Third Parties’ Impact Across the Risk Spectrum

From Scott Shinners’ “Effective Automation for Third Party IT Security Risk Management” session

Strategic risk – inability to achieve strategic objectives
- Selecting the wrong third party or selecting a technology that won’t work for your organization

Reputation risk – risk arising from negative public opinion
- Third party relationships that could damage the firm’s reputation
- Failure to monitor the nature or makeup of the ongoing relationship with third parties

Operational risk – loss due to inadequate or failed internal or external processes/systems
- Process gaps or errors caused by third parties’ process control failures

Transaction risk – third parties fail to perform or meet contractual obligations
- Third party delivery failure goes undetected without adequate means to remediate

Compliance risk – risk of noncompliance internal or on the part of third parties
- Third party systems that do not support the firm’s requirements for compliance with regulation

“Ensure that your cyber insurance policy covers your cloud service providers!”
Do you need something to do while in an endless stream of Zoom/Skype/Teams/etc. meetings?

Are you tired of the backgrounds you have to choose for these meetings (although, the galaxy backgrounds are pretty cool)?

Check out the North America CACS 2020 Virtual Resources for our downloadable coloring book, virtual backgrounds, #IAmISACA selfie sign, and more!
Industry 4.0: Future-Proofing Your Career Panel

Moderator: Pam Nigro
Panelists: Shannon Donahue, Jenai Marinkovic, Tammy Moskites

The professional paths many business technology professionals have traversed—IT audit, governance, risk, and security—are at a crossroads as automation and new technologies are changing the skills required to remain competitive. As automation increases, so must your technical skills, especially if your enterprise has increased expectations for expertise across broader subject areas.

“Now is the perfect time to demonstrate your leadership by spearheading a post-mortem on what went well and what didn’t when you switched to a remote workforce. What lessons were learned and how were security response scenarios handled with a completely remote team? Use this data to help establish an enterprise-wide cybersecurity incidence response plan focused on remote workers.”

— advice from step 6, Be a Leader.

Read more insights from the panel in this ISACA Now blog post that lists 7 steps you can do to help ensure your continued career growth.
Checklists and Questionnaires: Secure Partnerships

From Andrew Neal’s “Both Sides of the Coin: Being and Finding a Secure Partner” session

We’ve seen tremendous change in consumer expectations around data privacy, especially for global organizations. The consumerization of data privacy has put pressure on organizations. Many public companies’ boards are now involved with managing risk, are directing CEOs to ensure third-party risk is addressed, and even organizing the questions that get asked of third parties.

**The pros of checklist-driven security:** Can be automated, may be supported by various platforms, forces a common response set, aligned with internal risk framework, scoring may be automated as well, and can be outsourced.

**The cons:** May not recognize strategic vendor, lack of nuance, only a first step, and a bad answer does not equal bad security.

**The best answer is often**, “It depends. Tell me more about the question. Tell me more about the situation.” A lack of nuance can really limit the value of security questionnaires.

**Steps to put secure partnerships in practice:** Keep the questionnaires to a minimum, look past the answers to the programs, develop relationships and partnerships, provide resources to develop vendors, and remember, the goal is not a completed questionnaire.

What will the COVID-19 impact be?

- Will third parties that come onsite have to meet certain standards?
- Some vendors may be under huge financial stress.
- Will they afford the same security measures going forward?
- Baselines may also change in the future.
- What will employee and customer expectations be?

Assessing Risk and Information Security Simultaneously

From James Meyer’s and James Bothe’s “NIST Cybersecurity Framework Best Practices” session

- Even though there are two different owners for the process, if you shared the assessment time together, you’re addressing all of the functions in the security model and risk assessment.
- Vendor risk management can sometimes be an overlooked aspect of a cybersecurity program.
- The best programs we’ve seen in our clients have vendor risk management embedded.
- It helps to plan ahead for the activities you need to perform throughout the year, so that there are no surprises, and that tasks are evenly distributed.
- In all cases, you really need an audit process to make sure the inventory is accurate.
- A vulnerability management program relies on correct asset inventory.

- “Storming, Norming and Performing”
  - Storming—team disagrees
  - Norming—then reaches agreement
  - Performing—we know what we need to do, so let’s identify next steps
- Perform Table Top exercises annually to socialize the program; people who aren’t typically involved in security can learn their roles and responsibilities.
- Table Top exercises help participants appreciate what everyone contributes.
- Collaboration matters.
Tools to Secure the Cloud
From Andrew Weidenhamer’s “How Hackers Profit from Common Cloud Services” session

There are many applications organizations use daily that users may not realize use cloud platforms, such as Salesforce. Not all cloud solutions are securely configured; it’s not uncommon to find misconfiguration while doing a penetration test, and misconfigured buckets have led to high-profile breaches.

If you’re an auditor or an engineer, using a tool is very helpful. Here are some that you may find useful:

- **GitLeaks**—open sourced and easy to install; identifies sensitive data that might be stored in public co-depositories.
- **ScoutSuite**—open sourced and can scan your cloud environment looking for misconfigurations; supports all cloud platforms. One of the better free and open sourced platforms out there. It is comprehensive and can give you a good idea of how your environment is configured and whether you need to make any adjustments.
- **CloudTrail/CloudWatch**—CloudTrail is AWS’s tracking system. If you set up a CloudTrail on your S3 bucket, those logs will be sent to CloudWatch. You can set up alerts for certain events.
- **AWS Config**—a tool to ensure that your services are configured according to best practices, and warns of non-compliance.

Seven Deadly Signs of Negative Self-Talk—And Four Questions to Ask to Overcome It
From Sandy Silk’s “From Surviving to Thriving as an ‘Only’ in Cybersecurity” session

When you find yourself doing one of the following, you’ll know you’re caught in a loop of negative self-talk:

1. **Mind reading**—Assuming we understand what other people are thinking without any real evidence
2. **Overgeneralization**—Something always/never happens
3. **Magnification**—Exaggerating small negative events into disasters
4. **Minimization**—Dismissing our strengths and positive qualities
5. **Black/white thinking**—Interpreting anything less than perfect as a character flaw
6. **Personalization**—Taking responsibility for things outside your control
7. **Fortune telling**—Predicting a failure based on no real evidence

To disrupt your unproductive thoughts, try asking yourself these questions:

1. What is your evidence for and against that thinking?
2. If you were being positive, how would you perceive this situation?
3. If this happened to someone else, what would you tell them?
4. Is thinking this way helping you feel good or achieve your goals?

For more insights, read Sandy Silk’s ISACA Now blog post “From ‘Meh’ to an EPIC Career in Cybersecurity”
Attendees were able to meet the One In Tech staff and learn about its upcoming launch and goals. An ISACA Foundation, One in Tech works to build a healthy digital world that is safe, secure, and accessible for all. This includes: preparing the next generation to be healthy digital citizens; creating avenues to achieve a diverse workforce; and providing access to and education in technology. We can't wait to engage you in this important work! Stay tuned for more information coming soon.

A North America CACS attendee asks for more details about the One In Tech foundation during happy hour.

No Spoilers: Binge-Worthy Streaming

Attendees who wanted to share their favorite shows to stream had a lively discussion during the No Spoiler Zone happy hour. Here is the list for you to check out; also recommended is a new app, CatMouse, that offers free shows. Happy viewing!

The Act (and the documentary Mommy Dead and Dearest)
Afterlife
American Gods
Arrested Development
Avenue 5
Bandersnatch
Black Mirror (but maybe skip the first episode)
Boston Legal
Breaking Bad
Castlerock
Community
CSI
Deadwood
Dexter
Fear the Walking Dead
Fleabag
Insatiable
Justified
Killing Eve
Law & Order
Lucifer
Making a Murderer
The Mandalorian
Mrs. America
The Office
On Becoming a God in Central Florida
Ozark
Parks and Recreation
Penny Dreadful
Picard
Preacher
Run
The Seamstress
Silicon Valley
Six Feet Under
Sons of Anarchy
Space Force
The Staircase
Star Trek: Enterprise
True Detective (Season 1 is best)
Upload
What We Do in the Shadows (both the movie and the show on FX)
The Wire
“My job isn’t at all about making predictions; instead, it’s to reduce uncertainty. It’s about preparation, not predictions. Therefore, I don’t like to answer the question, ‘What is the future?’ My job is to create a state of readiness within an organization. As a futurist, I prefer to use a methodology—a strategic foresight framework.”

“Why do we have this constellation of smart things? Stop for a moment and think about all of the data we could capture from all these devices. Some may seem silly, like a smart microwave that won’t pop your popcorn if you haven’t logged enough exercise for the day, but there are real data concerns with sensors and their capabilities. What are the implications for the toilet that does urinanalysis, the glasses that take your temperature or track what you’ve been viewing, the ring that measures heart rate and oxygen levels?”

“I’m going off-grid, I welcome my microwave overlords.” – Bronson Y.

“Artificial intelligence is not just used to answer questions, but also in a generative way. They are starting to generate slightly different people to get around copyright laws. What happens if someone synths your CEO? It is already happening.”

“The future isn’t written yet. But we wind up creating problems when we passively accept what is happening and don’t inject ourselves in the process.”

“As a futurist, I don’t think about time in a line, but in a cone. You have to think about tactics and strategy while also looking to the future. You should be thinking about your role in the organization in the future. If you’re someone who works in compliance and security and risk, how does that evolve? It’s not just futurists that have to think about readiness, it’s also you.”

“I’m a huge fan of trying to spot risk very early in advance. If you can spot risk super early you can mitigate it or turn it into an opportunity.”

Deep uncertainty warrants deep questions.

• Who decided the systems and developed the baselines?
• Who owns your biometric data?
• Should you have a right to keep your emotional state private?
• What if your company wants to use behavioral biometrics?
• What does risk and compliance look like in a world where biometric data is constantly collected?
• Which government agencies set the rules for biometric data?
• How do we get our executives excited about data governance?
Social Media Roundup

Attendees loved sharing insights, their caricatures and their favorite sessions on social media. Search #NACACS on Twitter, LinkedIn and Facebook to see more!
Thank you to our sponsors!
You continue to be amazing partners, pivoting to a virtual event quickly and adding real value for our attendees.

Platinum Sponsor
[Image of AuditBoard]

Gold Sponsors
[Image of Galvanize]
[Image of OneTrust GRC: Integrated Risk Management]
[Image of Qualys]

Silver Sponsor
[Image of ServiceNow]

Bronze Sponsor
[Image of FastPath]

Supporting Sponsors
[Images of Patchworx, Canaudit, ISACA Central Maryland Chapter, RiskRecon, and Mastercard]

Ad Sponsor
[Image of Secret Double Octopus]

Visit [www.isaca.org/training-and-events/conferences](http://www.isaca.org/training-and-events/conferences) to view all of ISACA’s upcoming events, virtual and in-person.

We hope to see you soon!