Webinar

September 11th, 2025

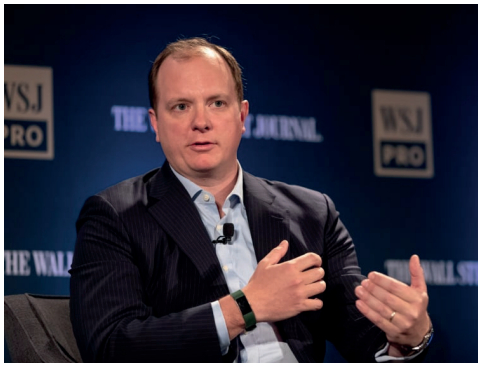
Report | **Transcript**

ACFE
Association of Certified Fraud Examiners

Chapitre français

Agile AI to the rescue of compliance and fraud risk management

Matt Galvin



He currently is a partner with Steptoe LLP which focuses developing data-driven risk management systems and helps complex organizations design global compliance programs and lead cross-border investigations using technology.

Matt served as the first-ever Counsel for Compliance and Data Analytics at the Fraud Section, U.S. Department of Justice, where he:

- Evaluated corporate compliance programs in enforcement,
- Advised on Compliance
- Monitors and their oversight,
- Assessed post-resolution improvements,
- Identified, designed and developed analytics tools to assist prosecutors to identify and pursue white-collar crime,
- Built out an analytics function to generate criminal fraud cases and support investigations and trials.

Prior to that, Matt was Chief Compliance Officer at AB InBev, leading global compliance efforts of this Fortune 200 company across 80+ countries. He also practiced for over ten years with leading international law firms.

Matt is a New York and Hong Kong qualified lawyer. He has held positions with Massachusetts Institute of Technology, Harvard Business School, Sorbonne Law School and Fordham Law.

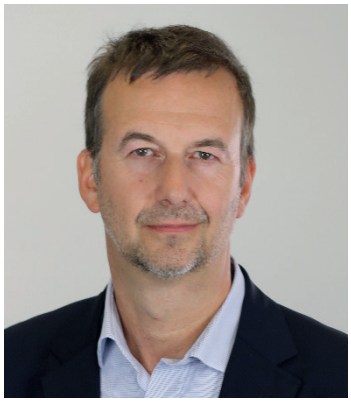
mgalvin@steptoe.com

Mark Button

Mark is the Director of the Centre for Cybercrime and Economic Crime at the School of Criminology and Criminal Justice, University of Portsmouth.
He conducts research on a wide range of areas for bodies that include the Home Office, National Fraud Authority, EPSRC, Sentencing Council, Cifas, Midlands Fraud Forum, Crowe Clark Whitehill to name some.
He also has an interest in private policing, security management and the regulation of it and has been involved in helping to develop the standards for this for the United Nations Office for Drugs and Crime.
He joined the University of Portsmouth in 1997. He was Associate Head (Curriculum) of the department between 2004-2012.
His research interests began with private policing with an interest in non-state contributions to policing. This led him to fraud where this is largely the case. Along that journey he has developed interests in Counter fraud, Cyber-frauds, Computer misuse, Fraud measurement, Security management, Private security regulation amongst others.

mark.button@port.ac.uk

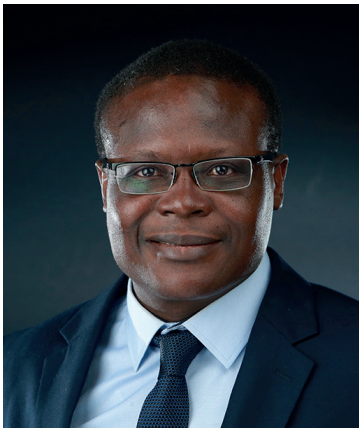
Laurent Colombant



Laurent has been helping financial institutions, commercial entities and governments tackle financial crime using NLP, machine learning and analytics since 1998. He has worked on sanctions screening, anti-money laundering, internal and external payment fraud as well as terrorist financing. He currently focuses on payment integrity which includes optimizing sanction filters and procure to pay process from supplier integrity (ESG), to maverick spend, to travel and entertainment fraud.
Prior to joining FortiComply Laurent worked for SAS Institute as a solution lead and for Cognitive Systems Europe (Temenos) as general manager of a team specialized in scanning and STP repair of SWIFT messages.
He holds an MBA in Finance from the University of Michigan and a joint degree in linguistics, econometrics and computing from the University of Montreal.

laurent.colombant@forticomply.com

Francis Hounnongandji



Francis, CFA, CFE, is a corporate governance and anti-fraud expert and financial advisor with deep expertise in data science, predictive analytics, artificial intelligence, machine learning, and emerging digital technologies.

He brings more than 25 years of international experience with global corporations, audit and advisory firms, and government institutions, and has conducted assignments in over 30 jurisdictions across Europe, the Americas, Asia-Pacific, Africa, and the Middle East. His work spans advisory and research in corporate governance, internal controls, fraud risk management, financial investigations, anti-money-laundering, financial advisory, and business and corporate strategy.

His commentary and editorials have appeared in leading international newspapers, including the *Financial Times*, *The New York Times*, *Le Monde* and *Les Echos*. He serves as President of the Institut Français de Prévention de la Fraude (IFPF) and of the ACFE France Chapter. He is editor and co-author of *Histoires ordinaires de fraudes* (Eyrolles Editions d'Organisation).

fh@ifpf.fr

CERTIFIED FRAUD EXAMINER

Judith Beckhard-Cardoso

I think now we are all set up, and you can probably hear everyone. I see on the on the chat that everyone is connected. Can I have someone on the chat tell me whether everyone can hear our panels. So, Francis, Matt, Laurent and Mark, we can hear. Brilliant. So, you are all good, guys. You can move on.

Matt Galvin

Looks like we have a fabulous global audience. Thank you everyone for joining.

Francis Hounnongandji

Okay. let's start. Thank you for joining and thank you Mark, Matt and Laurent for accepting to share your insights with us on this critical subject being the use of AI to Enhance compliance and fraud risk management. What I will start by asking you in turn, starting with Mark Burton, is to give us a 2 liner on your presentation related to this subject. Afterward I will ask you your bluff, your "bottom line up front" on this subject. We will spend 35 to 40 minutes approximatively with you sharing your insights and afterward we will take some questions and answers coming from the audience. So that will be it. Lets start with Mark, could you please give us a 2 liner, 3 liner of your presentation on your background related to the subject please.

Mark Button

Sure. So good afternoon, everybody. Great to see you all. I'm Professor Mark Button from the University of Portsmouth, where I'm co-director of the Centre for Cybercrime and Economic Crime. I've done lots of research over the years on fraud related issues. And obviously AI has increasingly come into that area both as a risk and obviously as a solution. And obviously we're going to talk a lot about the solutions today, but the risks are just as breathtaking when you look at some of the things that are going on.
But as I was told only two lines, I'll stop there and we'll come back to some more depth a bit later and I'll hand over to the others.

Francis Hounnongandji

Let's move to Matt, please.

Matt Galvin

Hi, my name is Matt Galvin. I'm a partner with Steptoe based in DC. Until recently, I was the first ever counsel for Compliance and Data Analytics at the US Department of Justice Fraud Section in the Criminal Division where I both led evaluations of corporate compliance programs and built out AI and other data analytic solutions to find and investigate white collar crime. I have experience in the private sector as the former Chief Ethics and Compliance Officer for AB InBev. I've also moonlight as a quasi-academic and help position at MIT and Harvard Business School. And I think my thesis today for the ACFE is that for in-house practitioners, whether you're in the audit, the fraud control or compliance functions, that the advent of AI and data analytics based risk management is blurring the lines of those roles in house, and I think quite often there's a lot of us looking at the same data with the same solutions to accomplish very adjacent things.

Francis Hounnongandji

Laurent, I will ask you to do the same, but in addition if you can give a quick definition of what we could consider an agile AI please.

Laurent Colombant

Okay. So, my name's Laurent Colombon. I'm a co-founder of a start-up called FortiComply. I've been working on software solutions for most of my career. It's 9.11 today.We didn't organize the conference today on purpose.. But I was running a company called Cognitive Systems when 9/11 happened and was one of the initiators of one of the firstsanction filters at the time. And so, I spent most of my career applying machine learning, analytics, NLP to detecting white collar crime, whether that's, SWIFT payments, internal fraud, procurement fraud and the likes. So, my take today is on AI is that it's something that can be very useful, very powerful.But you need to know how to set your projects up, not to end up with disappointing results to call it that way. Now to answer Francis's question about Agile AI I see it more as adaptable AI in the sense that we can see that contexts, the political geopolitical context, the regulatory context, the technological context are ever moving and I think that on the positive side of AI we can rely on its agility to adapt to the rapid pace changes.

Francis Hounnongandji

Thank you very much. I will not take time to present myself. My name is too long already, so my 2 liner is already taken. Let's come back to Mark Burton. You were alluding to some huge risks coming from AI, but also some of the solutions.What would be your insights regarding how Agile AI could help compliance and fraud risk management teams measure, for example, fraud risk with analytics, one of your key focus, and detect fraud or adhere to new regulations.

Mark Button

So, first on measurement, often people say you can't measure fraud, and I've done lots of research over the years in a whole range of different types of expenditure where organisations have been able to measure fraud. It's just that you need the resources to do that measurement, and you need to apply the appropriate statistical and methodological approachs. And in essence you can do it in anything where there are a similar range of transactions. So you can measure fraud on things like insurance claims, procurement, expense claims, …. You extract a sample of an appropriate size according to the total population.

The population is to take a random sample, you investigate those and then you can come up with a percentage of loss within a range of statistical confidence and range. And that's been done in a number of sectors for a long time in a very traditional, if you like physical way.

And to just to give you some numbers, the last time we did analysis of organisations that have done this, we had an average across all those fraud loss measurement exercises of 6 1/2% with fraud and error that included error in some of those.

And that's a significant number. And that's obviously a real number built on real exercises compared to say the ACFE number where you just ask how much fraud you think you've got, say 5%, it happens to be in a very similar ballpark. So, people's finger in the air is not too dissimilar.

Francis Hounnongandji

Ok.

Mark Button

But obviously with modern technology and AI and things like it I don't think it's long before we have a situation where you have the ability to utilise AI to investigate a sample and come back with figures and assessments, it's just the breathtaking pace of AI is such that I just think that is something that is going to be highly likely.

You know, in the next 5-10 years that we'll be able to much more accurately measure fraud. And I think that will be a game changer because probably a lot of the people in the audience here today struggle with going to senior decision makers to make a case for Fraud being an issue that warrant significant investment. Often the answer is t built on "we don't have much fraud" and that's we don't have much fraud because we're not measuring fraud, we're just looking at the detected cases relates to how much activity you put in.

So, I think once we get to a situation where we do have that ability to measure fraud with AI that will I think free up a lot more resources to target this problem. Once you have a problem in an organisation that has a clear cost that enables a clear strategy to be developed with the appropriate resources, with obviously a link to a return on investment to tackle that problem. So, I think a AI opens up a lot of opportunities to accurately measure the problem in the future and other related problems using similar methodologies.

Francis Hounnongandji

Thank you very much. Let's move to Matt.

Matt Galvin

Yes, no, I think I agree with pretty much everything Mark said, including what the premise that is." You can't start to really address a problem, whether it's in corporate culture or life, until you admit that you have one". And quite often, the work is done to identify where you might have risk, where you might have fraud. And quite often, fraud comes at the same time as regulatory and compliance risk. If fraud is big enough, it can become a security issue for a large company.

If the fraud is contagious enough, it can easily become a bribery or a graft issue for a company, and there are many sister problems to the problem of fraud. The only thing I might challenge Mark with is the speed at which things are moving and allow for metrics in measurement of fraud or compliance risk. I think the movement towards data-driven fraud prevention and regulatory compliance programs creates a ton of opportunity to measure risk profiles. And I think the first piece there is, at the outset, accepting that you have an issue. One of my favorite things about working with fraud groups is you start with the premise that there's fraud in organizations.
Because, often, with legal or lawyer groups, you start with the imaginary premise that legal companies, organizations have no legal problems. Everything is fine, there's nothing to see here. But if you move away from that premise into the compliance, ethical side of it, the fraud side, you start to see the goal of risk managers isn't to eliminate it entirely. That would be a nice objective. It's to identify it quickly and to identify it before it metastasizes into something that can both poison the culture, become a legal issue, become something that you can't recover from.

And I think the challenge that we have from an analytics standpoint is quite often our analytics are driven by outliers, which by definition are things that have metastasized. And so, as we go, and this is where I think the evolution of the detection is going to coincide with the ability to look at more.
More than 80 thousand factors of a fraud outlier into 800 thousand of different factors that are preconditions that led to it. We'll both have metrics for risk factors and we'll have metrics for cultural indicators of when fraud might happen.
And I think we'll move from metrics through continuous monitoring into prediction a little bit sooner than we think for companies that have a higher degree of maturation, both in terms of their systems and the way that they can apply them.

Francis Hounnongandji

Thank you very much, but Laurent.

Laurent Colombant

Yes. So, it's always a little bit difficult to speak after two speakers like Matt and Mark and add something. But I'll throw some things into the conversation, I mean.

I worked for a very large petroleum company, UK based, and interestingly the CFO there said the only thing that really kept him awake in terms of risk was fraud, and what he used to say was that it was like a shark. A shark could be lurking under your surfboard. It could nibble a finger off, a hand, an arm, or just outright kill you.
Now the image goes a little further because if you're surfing off of Cape Town in South Africa or Brisbane in Australia, you may be running more of a risk of meeting a shark. It's a little bit like being in the construction industry. There's a a higher likelihood of there being sharks there.

So it is something difficult to measure, but you have to measure it in some way or fashion. Now, AI does help you measure outliers, as Matt said. So, there's models like outlier
models, clustering, all sorts of,models that you can develop that can mathematically determine what's outlying and the value of those outliers. That being said,

I don't think that you can cut the human being out of the decision loop because there's always a call to be made about a machine generated alert, and I'm not a lawyer, as you can hear, but there's always a call to be made as to whether this is an error, a fraud, waste, if it's a misinterpretation of contract. So, there's a lot of things that come into play for me in the measurement itself and maybe the last thing that I'll throw into the conversation is the . garbage in, garbage out story. What I love about meetings about analytics, fraud and compliance is that in the first two minutes, somebody says garbage in, garbage out, and then you spend 58 minutes talking about how you're going to analyze the data. What you need to know is today AI can be used to clean data and I think that's something that's not spoken about enough because you've all heard about neural networks, link analysis, those are good at surfacing collusions, for example, to surface bid rigging, for example, but you can use the same exact technology to make sure that Mark Button, B-U-T-O-N, Mark Button, B-M-A-R-C, Mark, M-A-R-Q-U-E Button are three individuals or are the same individual by combiningdate of birth,address and other contextual information in there. So, I think that's something also that's maybe underestimated today is maybe the power of AI to clean the data that's needed for fraud detection or compliance.

Francis Hounnongandji

Ok. Thank you very much, Laurent for this. Let let's move to the regulatory compliance side with the changing

political and geopolitical landscape. What are the trend you are perceiving? And how can AI help in this upfront to start with? Now let's start with Matt.

Matt Galvin

No, I appreciate that. I think,, certainly I sit in the US and it's difficult to say that regulatory enforcement or prosecution enforcement of white collar crime is up.
Certainly, I think with any change of administration, there's a resetting of priorities and that can create, some change of velocity of certain cases and movement.

With that, it remains to be seen what's going to be happening in the next six months if it's going to follow normal trends. But what is certainly happening is there's a technological AI revolution in risk management and what's certainly happening is if you think of the lifespan of cases, the point in time that a case is evaluated by someone like me, tends to be towards the end game of an investigative regulatory proceeding, and I think what always happens in that the people doing that evaluation, they're going to be human and they're going to be very much influenced by the technology available to them on the day that they're evaluating that program. So, what you should be thinking about is how will your program age over timewhen it actually would come under some regulatory or prosecutorial review?

And I think the answer to that is thatthe expectation is almost certainly going to bethat your system needs to be data-driven. It's just inevitable.
Now I think the other piece of that is there's more opportunities for prosecutors to use and government agencies to use LLM (Large Language Models) or AI (Artificial Intelligence) or different advanced modeling techniques to help them identify and pursue crime. Now that was a big part of what I was doing when I was in the government in the fraud section. And so, you simultaneously have this ability to make the distillation of global information much less expensive that makes data usable and you have around the world increasing transparency and initiatives or NGO driven or government driven initiatives that create huge amounts of data that can be harvested.

And whether that's in the corruption space about foreign government procurement or the algorithms that Laurent was talking about that make bid rigging or specification rigging or collusion discernible from an algorithmic basis.
Those are often indicators of corruption too. So, in the FCPA or foreign bribery space, I think the ability for prosecutors to quickly distill and triangulate areas of risk without having to go through the company or through traditional investigative techniques to get there.
I think that's also changing the landscape. So, I think all what that means to folks in-house is, well, the prosecutor, the prosecutorial climate is such that I need to advance technological wise and you're probably getting pressure from the business to do that too.

But in the short term, probably no one, the chances of someone looking is relatively low. So, it actually affords a great opportunity because one of the hardest things to do when you're an in-house risk manager is remove process. But if you think of a data-driven program as being able to look at effectiveness and then if you say, what data I can look at then I'm really expected to look at a much greater array of risk. Meaning now is an excellent time to pivot intoa more data-driven program, be that much more driven towards effectiveness, be that much more driven to manage the next regulatory moment when you'll need it.

Francis Hounnongandji

Thank you, Mark. What would you like to add?

Mark Button

Yes, I think I'd agree with much of what Matt just said. I do think the key thing is that the world is a much more complex place with so much going on in terms of regulations and compliance and related issues. If you just look at the sanctions post Ukraine war, there's been so manymore issues that companies and organizations have to be aware of and be concerned about in terms of the people that they're doing business with that the complexity combined with all those other factors just naturally drives an organisation to technological solutions because I think that is the only way to aid and enhance compliance is by utilizing some of these products that are available. It's just too complex without that so, I think that's what I would say on that issue.

Francis Hounnongandji

Laurent what about you.

Laurent Colombant

I'll just add on to what's just been said that there's a lot of change. I'll take one change that interests bankers these days in Europe. There's a the new fast payment regulation which means that you need to process any payment in a wider zone than SEPA under 10 seconds. Now obviously payments, cross-border ones in particular, SWIFT payments need to be scanned against sanctions and other lists and there are false positives in the automated scanning process. So, optimizing that is already going to become even more crucial than it was before because the regulatory pressure for efficiency in payments pushes the bar up that much more.

Now, to Mark's point the PEP list, I mean politically exposed people list, there's over a million people in there and the rate of change of that list used to be like 10% per annum. It must have been 30 to 35% last year. So, how do you cope with that without technology? Now on the new Ffontier of technology, what I see is that historically there were a lot of issues detecting things like pre-contract award, bid rigging, that was a hard one to crack because there's a lot of negotiations and paper involved in that process. There's the RFP, the RFI, there are several negotiations. Now with text analytics and LLMs (large language models), that becomes possible. What we could not do before is now possible with large language models.

Now I love saying the opposite of what I just said. I get the question, which is why doesn't ChatGPT find fraud? Well, ChatGPT is really not that good at finding fraud because ChatGPT is generic. See, it looks at everything. It looks at Shakespeare, it looks at how to repair a car and it's also going to look at how to bake a cake when what you ask is a question about fraud.
It doesn't have the expertise that everybody on this call has, nor the context of what it's supposed to do. So, that would be my little curveball on the topic.

Francis Hounnongandji

Okay. Coming to one subject when we speak about fraud risk management that also involves investigation, and prevention. I want to focus a little bit on the evolution of fraud modus operandi across the time and across geographical areas, because one scheme that you will find in one region will be influenced by culture, the reasons behind a regulation and operational systems.
How for an international company, for example, can we use AI to take care of those changing and moving targets and fraud schemes?
And the second thing regarding investigations, what we are focusing on at the end is proof and proof admissible

in court. That's our premises when we run an investigation, at least proof admissible in front of the authority which will have to make the decision regarding the findings. First, how could AI be used to take care of this evolution of the modus operandi across region and across time? And second, we come to the investigation part and the proof because today using AI, we can fabricate proofs or tamper with them, create video, generate a document that will look exactly the same as an actual one, except that we could have some.
Technical tools to identify those. So, I will start with Laurent. How do you see the impact of AI to take care of the evolution of the modus operandi and then the quality of evidence?

Laurent Colombant

Yes, I touched upon it a little bit on the bid rigging and pre contract award. So, for example, that's a type of fraud that is well documented. You know, scholars have very precise statistics about it. It's been looked into now addressing it from a technological point of view has become a lot more efficient now bid rigging in construction projects for example, or high capital spend projects are rife with issues.

Pre-contract award, price fudging, market sharing and all that, that's a new frontier addressable with advanced analytics where it wasn't so much possible in the past. Now the fact that we can ingest high amounts of data and process them with models means that you can look at a million SWIFT payments; you can look at 200,000 invoices in a matter of hours. Now the AI component to it has made it more efficient, I would say, in identifying specific modus operandi and reducing, the false positives which have always been an issue in any AI or analytics tool now.

In terms of how do you substantiate evidence? There again, there are interesting solutions for auditability and traceability. I mean I'm not a lawyer. I do investigations and sometimes people just tell me what you've put together is not receivable. So we've thought about this. For example, you can write evidence to the blockchain, which is a technique that is worthwhile looking into and if you don't know what you're looking for, because often in fraud that's the crux of the matter (in the beginning of an investigation you don't really know what you're looking for). As Matt said, some people are work on the premises that there's no fraud and on the other end of the spectrum, sometimes the premise is that there's 10 to 15% of fraud.. And it's rife with fraud, fraud lies a little bit in the middle, but the solution could then be to write all of the data to the blockchain before even analyzing it, which is also I would say a technical capability that can be used. That way after the fact you can say that this document was a specific document and not another document. And you can prove that it's been tampered with or not 10 years later.

Francis Hounnongandji

Thank you, Matt. What's your take on this point, namely the evolution of the fraud Modus Operandi?

Matt Galvin

I love the provocation and I agree. No, with this, because when you were starting, I thought one of the first things you were saying would be, Matt, how would you commit fraud in the age of AI? Because it's a really great moment to be a fraudster. It's a really great moment to have deep fakes.

Francis Hounnongandji

No, no.

Matt Galvin

People transfer money and impersonate worth, right?. One of the first days I did a fraud section to be a bit of a rabble rouser we prosecuted healthcare issues and diversion issues and I produced 40 patient profiles in 30 seconds of patients records that would justify the prescription of opioids to create a paper trail for someone that was diverting narcotics from the legitimate supply chain. I think we live in an age where authenticity is going to be a currency that's under threat. I share Laurent's vision because I think you need some potentially distributed ledger solution that you could trace back digital items to, a source, whether that's achievable or energy efficient, I think is another challenge, but I do think it's a problem and coordinate of a solution. And so I think that one hand you need to educate your workforce as a risk manager of precisely these risks.

I think in the same time there's increasing challenges of how to manage the internal risk and one of the things I was really worried about in the department and we had a whole AI initiative relevant to this topic, and it came out in the evaluation of corporate compliance guidelines, is how are you supposed to manage the risks of AI within your organization?
I think it is quite easy to imagine you could set up a securities trading bot that if you are not instructed it in certain ways, it would quickly find that front running was highly profitable. It would quickly find that by reaching through different sectors of information that would otherwise be off limits.

They could trade on inside information, which is an excellent trading strategy, but for the fact that it's illegal and in a world that AI might do that, who is accountable for it and how do you manage that risk in a key focus? How I looked at that was to drive some degree of accountability over AI within our organization and then beginning to see more mature organizations as they unleash AI because to fail to do that it will happen off premises out of the line of sight and to have solutions that you look at how AI is being used and have AI help you translate its use cases, and then you have some risk management function to see how it's being used in an organization, and that's increasingly becoming necessary as agents are passed with different corporate functions. And I think what is probably going to drive that is less the idea of risk, except in time of crisis, and more efficiency and more as people get smarter with the use of AI.

How do you capture that value? Because it is quite possible you have certain employees that will spend 5% of their time doing AI that would take 100% of their own job and fish. And you're like well, geez, I should have you do ninety-five other things with your day than fish. And how do I capture that?

That will drive transparency and how AIs going to be used and I suspect that will drive in some respects in more mature organizations depending what muscle's stronger than that visibility about how AI is being used.
But I think if we join forces with the folks that care about that in an organization, we will also find better ways to manage the accountability risk, the fraud risk. And simultaneously we'll all be learning hopefully at the pace of the fraudsters, how to detect external fraud risk.

Francis Hounnongandji

Mark, you were indicating some significant risks of coming from AI and also the andidote. So I'm assuming that you were thinking of the evolution of fraud schemas.
Now, could you please outline some of the key features you are seeing regarding this point?

Mark Button

And we can see that already. You know Matt mentioned the Hong Kong case where the finance person is thinking they were talking to senior directors. But you look at where AI is going and obviously particularly

things like agentic AI where we're going to have an AI person looking after our affairs. I will, or someone like me in the future will, come back into their office and the AI would have had an invitation to speak at a conference. Yes, I would have accepted that conference, negotiated a fee, booked my flights and that all sounds wonderful in the sense that, I'm going to have this done by a helper of the future. But one can also see how that will get exploited by the criminals. On the other hand, you're going to have criminals targeting those AI agents.

With ventures to tap into my bank accounts, you are going to have criminals setting up agents to actually conduct fraud and tallied up with the best knowledge, the best data, etcetera. But like all of these things, we will then think of solutions to counter all of these things. So it's an ongoing process of evolution and arms race. And that's something I don't think we'll ever escape. But coming to the second part of your question about usability for courts and things like that, I think already there is a challenge, with courts accepting data, particularly in some jurisdictions, that has been untouched if we say by a human hand and it doesn't exist in a physical form. Courts are often behind on these technologies in many jurisdictions.

And again, you can think of how particularly Agentic AI will be able to help an investigator put a case together, put all this stuff together and then boom, we take that to a court and lawyers, good lawyers, hired by the bad guys, find ways to unpick, what the technology has done. In the face that our traditional regulations are all designed around people and not around technology. So I think there's still a lot of challenges with using that technology for criminal prosecutions. But, let's put it in perspective. You know, everyone in this probably knows that the vast majority of cases don't go to find their way to a Criminal Court. They're dealt with by alternative means where that probably is not as strong because we would probably like a lot more cases to go to the criminal courts.

Francis Hounnongandji

Very quickly because we are running out of time, and there still is one critical point on my list of things to discuss . I'm sure you have seen a couple of weeks ago, MIT published a report on the success rate of Gen AI project in corporate setting, concluding basically that 95% of those projects fail to deliver any value added to the those corporations. Quickly from your perspective and experience, what are two key recommendations you would make for data-driven projects to be more successfull?

Matt Galvin

Yes, I think that I guess there's a couple Silver Linings. One, I think that since the majority of AI programs and organizations are not fraud or compliance related, the majority of the failure is outside of fraud or compliance and we can learn from mistakes that people are making in those projects. But Okay. I'm sure the first person that ate a lobster probably got food poisoning, but that didn't make it a bad idea.
I think , we're learning very quickly how to engage with this technology as well, I mean it's been around for 10 years or so, but it's only been available in mass market for two or three year.
And I think you see errors of people making ittoo expensive and then it gets misused. I think you see errors of people making it too narrow and then it gets boring and not useful. And I think the smart organizations are moving towards that Goldilocks zone of thinking through cost-effective and also well-structured solutions of data inputs that's subjected to an LLM.

They're doing that in a way that's secure, that can manage confidentiality, that can manage all the information security risks that people might have. And then they are asking better what often prompt engineering or they're asking the right questions.

AI is not a genie. You can't just make 3 wishes generally and get something. You can get medium level work, but you're not going to get excellence; but I think used as a tool to drive towards excellence will help people get over that normal technological adoption hurdle where you have all this promise, then you have a period of disillusionment, and then you have a sober, steady progress throughout. And I think it's that mass group of sober, steady progress that I'm seeing a lot with the folks that I'm working with and the projects that I'm on, that we didn't say we're going to do everything with AI, but we're going to accomplish these tasks, that this is now possible, that we can shortcut this piece and we can set up interconnected systems that are working well together while maintaining visibility and how it's going to work. And so, I'm very bullish in the opportunity.

Francis Hounnongandji

Laurent, a very quick recommendation?.

Laurent Colombant

Yes, I'll loop a little bit to what was said previously. I do think that when you say it fails, at least in fraud and compliance, I think you need to measure where you are starting from.
So, you do need to know what your level of fraud is, what your level of non-compliance is, because if you apply a new technology or an optimization or a securization tool, if you want to measure if it succeeds or fails you definitely need to benchmark it correctly at the beginning. I can't insist enough on that point
And the reason why we do those bnechmarks is precisely to figure out what's not working with the AI. I'm not saying there's a silver bullet to all of it, but I would say apply it to cleaning the data.
You know, clean the data because AI is just as good as the data is, large language models go haywire because there's a lot of junk out there and it's just ingesting it and, statistically analyzing it and then maybe the last thing that I would add is I found that AI projects in the fraud space in particular open a whole can of worms of reflection about what is fraud. What is an error? What is waste? What is abuse? What is price fudging? Is that fraud? I've even heard, and I'm not going to say what company I heard it in. There was a category called "allowed fraud". So, everybody knows it's fraud. So, to measure the success of an AI project in this area, I think that you need to look at those things closely.

Francis Hounnongandji

Excellent. Thank you very much. We are going to move to the questions and answers session. Judith, you are monitoring the questions falling in the questions' basket. Could you please share some critical ones with us? We have 8 minutes.
By the way, Judith Beckhard-Cardoso is the lady spamming you and supporting us prepare the webinar!

Aissatou Ndiaye

Ok. Thank you very much for this.
We thank you very much. I learned a lot. I'm an internal auditor and a CFE. So, my question is how is agile AI shifting compliance from a reactive function to a proactive risk management tool in our work?. Thank you.

Francis Hounnongandji

Matt, would you take this one?

Matt Galvin

I think by and large, yes, because what happens, I think first off, compliance traditionally was really a set of processes to blend documentation so that when something went wrong, you had evidence that as a corporation, you tried to solve it. Now that's not preventative. That's basically an elaborate legal defense, and there's still a role in that. I think companies should still try to do the good thing and evidence that they're trying to do that. But what happens with data and what happens with audit is you have the capability now to get information closer to real time. An audit and risk management need not be like oh, I'm going to set a rule, I'm going to let people know, then I'm going to audit backwards against the rule and see how.

Behavior was then I'm going to change the rule and I'm going to do it again. You create the opportunity for more real time monitoring, for more real time interaction, for more real time, but behavioral influence. But as you build up those data sets what you get then, as Mark was saying at the outset, is statistical probabilities of what might happen next. And not only do you move away from being reactive, then you can go past continuous monitoring, and you can ideally move more towards predictive and pre-emptive. And I think, as I said at the outset, there's a blurring of lines between audit and compliance, but there's also a blurring of lines between audit, compliance and control because you're moving more towards what's happening now. And how do you prevent what's happening before? And how do you identify something, as I said earlier, before it metastasizes into something big? That feels much less reactive to me, but that's the enablement of data-driven risk management.

Judith Beckhard-Cardoso

We have two more questions. Yes, sorry, Francis. There are two more questions, one from Olivia Mola.
What action should be taken to analyze false evidence?
Management has a responsibility to consider as it is important to invest in tools that can authenticate evidence. It is important to keep this point in the risk assessment review and take action to mitigate it step by step. The organization should strengthen its digitalization program to avoid paperwork, for example, encouraging system approvals instead of signatures, or encouraging fingerprints instead of manual approvals, taking into account all the preventive and detection controls linked to identity fraud schemes, etc.

Francis Hounnongandji

It seems like a contribution to the debate. Thank you very much Olivia. We are going to close. Thank you.

Judith Beckhard-Cardoso

Exactly. Yes, Yes. There is one more, one more question from Angela Kroboth.
What is the best way to get started to integrate AI into your compliance or audit program? And I think that that's a great question to end it. How do you start? The path to getting where I am to where you are.

Laurent Colombant

I can answer really quickly on that one. Just I would, I would go step by step. I would like to find an area of fraud or a modus operandi where your maturity is low. Where you have motivated teams, that's two; and where you have accessible data, that's three. If you have those three things together, I would start by that corner of the organization.

Matt Galvin

I think that I would add that that generally makes sense, right? You need those three things. And often I work with folks and we're either doing a broad-based risk assessment that has a capability assessment that looks for those things for opportunities. Others intuitively have a sense of that and there's a clear problem they need to solve.

And they're like let's solve, Matt, can you help me solve that problem using some of these tools? And then we can use that to win hearts and minds that we should do it more broadly. So, I've seen both approaches broad to narrow and then narrow to broad.

Francis Hounnongandji

Ok. Thank you very much, Laurent, Mark and Matt. Thanks a lot. Thank you Judith for all the support. For those who will need a CPE certificate, please send in now a request to events@ACFE-France.FR, so that we prepare one and send it to you. Please make sure you have your first name and your last name clearly spelled in this e-mail so that we can send it to you.

We will compare with the record and if it meets the requirement, we will issue one CPE credit and send those to you. Next event will be on the 1st of October we are going to have a webinar this one in French, regarding geopolitical risk and governance in this unstable landscape. On the 9 of October, we are going to have a free 3-hours event in Paris on internal fraud and reputational risk management. So, you are going to have the invitation, at least for those on our distribution. Thank you very much for taking your time to attend. And again, thank you all the speakers for making yourself available and share your insights with us. Bye, bye.

Judith Beckhard-Cardoso

Thank you everyone and if you would like to contribute in any way or if you have any idea to make these sessions or have subjects to propose, please don't hesitate to spam me back.

Thank you. Thank you, Matt. Thank you, Laurent. Thank you, Mark. Thank you Francis. And speak to you guys soon. Bye, bye.

Definition of Agile AI for Governance and Fraud Risk management (Derived from the Panelists' Insights)

by Francis Hounnongandji, CFA, CFE

Agile AI is a form of artificial intelligence designed to adapt continuously and rapidly to changing contexts—regulatory, geopolitical, operational, and technological—while enhancing an organization's ability to detect, prevent, and respond to fraud and compliance risks.
It combines the analytical power of modern AI (machine learning, NLP, LLMs, outlier detection, clustering, entity resolution, etc.) with a design philosophy centered on flexibility, iterative improvement, and responsiveness to evolving risk signals.
Based on the speakers' insights, Agile AI can be defined along the following core dimensions:

Adaptable to Constant Change

Agile AI is built to respond quickly to dynamic environments. Laurent Colombant explained that regulations, political conditions, and technologies are "ever moving", and AI must remain "agile" to stay effective.
It absorbs new data, new fraud patterns, new sanctions, and new geopolitical pressures without requiring full redesigns.

Able to Learn from Evolving Fraud Modus Operandi

Fraud patterns evolve across time, sectors, and geographies. Agile AI supports this by:
- ingesting large and diverse datasets (invoices, SWIFT payments, text documents),
- detecting new patterns via clustering and outlier detection,
- adapting statistical models as behaviors shift,
- using LLMs and text analytics to uncover patterns previously inaccessible (e.g., bid rigging, pre-contract manipulations).

It reduces dependence on fixed rule sets—essential in environments where fraudsters constantly innovate.

Flexible, Incremental, and Practical Deployment

Agile AI contrasts with rigid, monolithic AI projects that often fail. It:
- focuses on starting small,
- selecting areas where data exists,
- working with motivated teams,
- delivering value in incremental improvements,
- and integrating human expertise throughout the cycle.

This is reflected in the panel's advice: begin with a narrow use case where maturity is low but data is available.

Enhanced Data Quality and Data Cleaning Capabilities

A unique aspect emphasized repeatedly is that Agile AI doesn't only analyze data—it cleans it.
Advanced AI can resolve entities, correct variations, and reduce noise.
This makes Agile AI superior to traditional analytics tools that assume data quality instead of repairing it.

Designed for Proactive, Not Reactive, Risk Management

Agile AI supports near-real-time monitoring and predictive capabilities.
Matt Galvin explains that Agile AI enables organizations to:
- move from post-incident auditing to early detection,
- assess risks before they "metastasize",
- shift compliance from documentation-heavy defense to continuous surveillance and intervention,
- eventually reach predictive and pre-emptive risk management.

This end-to-end adaptability is at the heart of the "agile" label.

Anchored in Governance, Accountability, and Human Oversight

Agile AI includes safeguards to manage the risks created by AI itself:
- ensuring AI usage is transparent and monitored internally,
- maintaining human decision-making for investigative judgements,
- securing audit trails (e.g., using blockchain for evidence integrity),
- preventing AI-generated false evidence or internal misuse (e.g., rogue AI trading bots).

Agile AI acknowledges that "AI is powerful, but not a genie," and therefore requires responsible deployment.

Built to Support Regulatory and Prosecutorial Expectations

Agile AI enables organizations to meet regulatory expectations that are increasingly data-driven, especially in fraud, sanctions, payments, and bribery enforcement. It is designed to withstand regulatory scrutiny because it:
- documents decisions,
- integrates auditable data flows,
- adapts to new global transparency requirements,
- and climbs in maturity as enforcement becomes more technologically sophisticated.

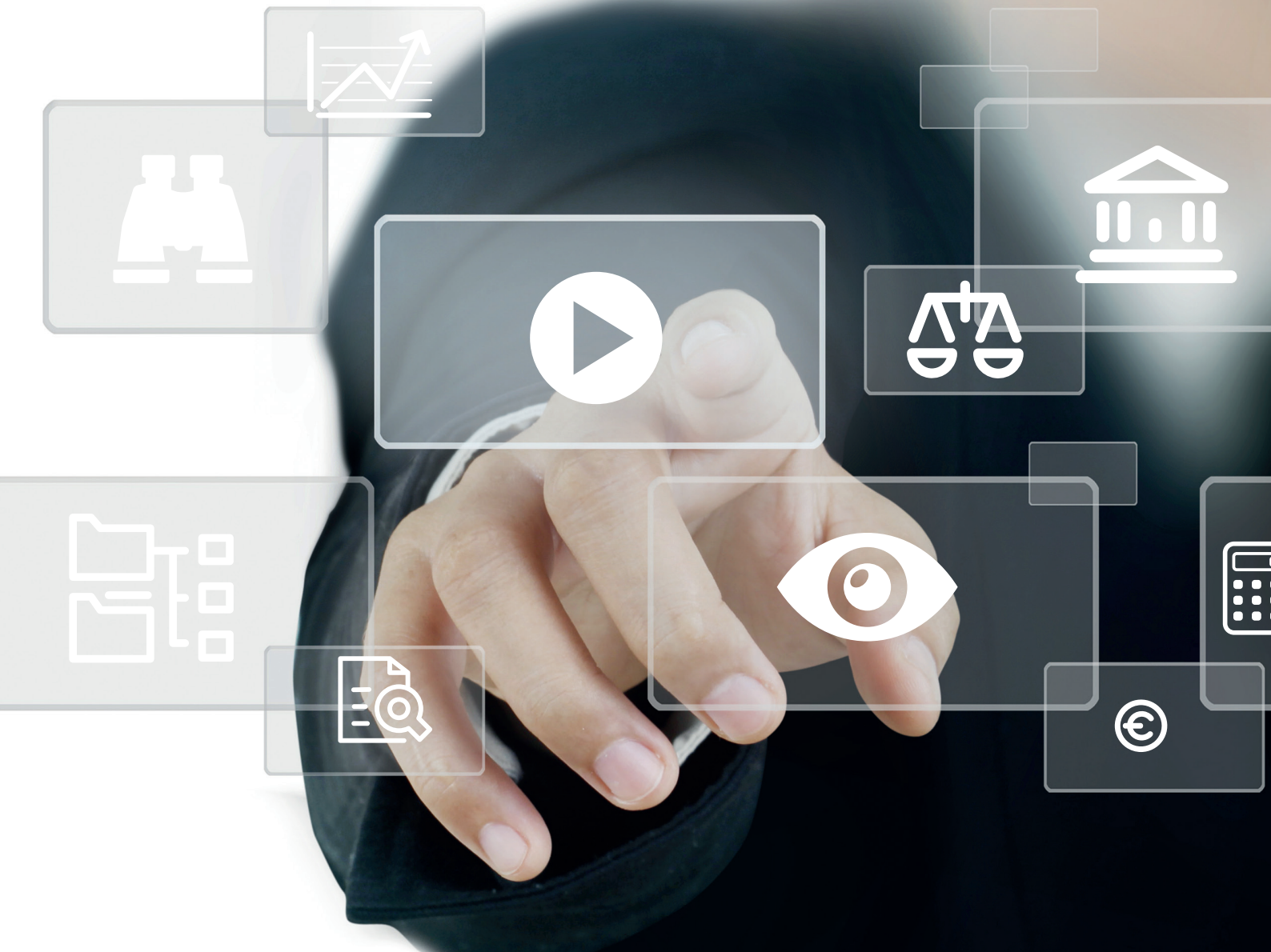
Final Synthesized Definition of agile AI

Agile AI is a responsive, adaptable, and governance-anchored approach to artificial intelligence that continuously adjusts to evolving fraud risks, regulatory pressures, and operational environments.
It leverages flexible models, advanced analytics, and strong human oversight to measure fraud more accurately, detect new schemes, clean and interpret large volumes of data, and shift compliance from reactive review to proactive and predictive risk management.

Become Certified Fraud Examiner®

The CFE is “in-demand…one of the most marketable credentials today”.

Robert Half International



www.ifpf.fr

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS · CFE ·

ifpf INSTITUT FRANÇAIS DE PRÉVENTION DE LA FRAUDE