

# Ethics in Information Technology

I am sitting down to write this column in mid-August, which, believe it or not, is quite late for an *ISACA® Journal* vol. 6 column (at least for me). The reason? After 3.5 years and 21 articles, I have decided that this will be my last column. I have enjoyed my time here but believe it is time for a new challenge and a fresh voice. As this is my last column, I needed time to think. What is the essence of IT auditing? How would I sum up IT auditing in a few words?

I believe that, fundamentally, good auditing, as with many professions and indeed life itself, comes down to ethics. Certainly, ISACA® has recognized this and developed a Code of Professional Ethics.<sup>1</sup> Further, we know that the culture, ethics and behavior of individuals and of the enterprise are

often underestimated as factors in the success of governance and management activities.<sup>2</sup> But I would go a step further and say that good IT auditing comes down to understanding the ethical implications of the information systems we audit. So, how can IT auditors influence the creation of ethical information systems?

## The Ethical Operating System

The Ethical Operating System (Ethical OS) has been designed to facilitate better product development, faster deployment and more impactful innovation, all while striving to minimize technical and reputational risk.<sup>3</sup> It does this by identifying and defining a number of risk zones (**figure 1**).

**Figure 1—Ethical OS Risk Zones**

Risk Zone	Description
1	Truth, Disinformation and Propaganda
2	Addiction and the Dopamine Economy
3	Economic and Asset Inequalities
4	Machine Ethics and Algorithmic Biases
5	Surveillance State
6	Data Control and Monetization
7	Implicit Trust and User Understanding
8	Hateful and Criminal Actors

Source: Adapted from the Ethical OS Risk Mitigation Checklist, Institute for the Future and Omidyar Network, [www.iff.org](http://www.iff.org)

Each of these risk zones are, in turn, evaluated by utilizing three prescribed tools.

### Tool 1: Tomorrow's Risk, Today (Risk Scenarios)

The first tool identifies a number of risk scenarios for each risk zone. These are intended to inspire a conversation about the growing responsibility and opportunity organizations have to manage social risk areas and anticipate longer-term consequences.<sup>4</sup> Each scenario also has a signal or a specific example in the present of something that might influence or shape the future. It is a clue as to how things are already becoming different.<sup>5</sup>

For example, under the risk zone 4, machine ethics and algorithmic biases, an identified scenario asks one to consider if one is ready for a world in which:



**Ian Cooke**, CISA, CRISC, CGEIT, CDPSE, COBIT 5 Assessor and Implementer, CFE, CIPM, CIPP/E, CIPT, FIP, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt

Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has over 30 years of experience in all aspects of information systems. Cooke has served on several ISACA® committees, was a topic leader for the Audit and Assurance discussions in the ISACA Online Forums, and is a member of ISACA's CGEIT® Exam Item Development Working Group. Cooke has supported the update of the *CISA® Review Manual* and was a subject matter expert for the development of both ISACA's CISA® and CRISC® Online Review Course. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules and the 2020 Michael Cangemi Best Book/Author Award. He welcomes comments or suggestions for articles via email ([ian\\_J\\_Cooke@hotmail.com](mailto:ian_J_Cooke@hotmail.com)), Twitter (@COOKEI), LinkedIn ([www.linkedin.com/in/ian-cooke-80700510/](http://www.linkedin.com/in/ian-cooke-80700510/)), or on the Audit and Assurance Online Forum ([engage.isaca.org/home](http://engage.isaca.org/home)). Opinions expressed are his own and do not necessarily represent the views of An Post.

*"[A] major social network company purchases a top US bank and becomes the first social credit provider. It bases mortgage rates, loan approvals, and credit access on deep data collected by its social platform. It takes into consideration the credit histories of close friends and family, locations visited (including frequency of visits to places like bars and legal marijuana dispensaries), and 'semantic analysis' of messages and photos to indicate whether individuals are generally happy, angry, anxious or depressed."*<sup>6</sup>

The signal provided is a company called Rex Homes, which uses data modeling and machine learning to match sellers and buyers of homes as accurately and speedily as possible on Zillow, Google, Facebook and more.<sup>7</sup>

Going forward, IT auditors can use these scenarios when assessing risk in the IT audit universe<sup>8</sup> or when defining an audit objective.<sup>9</sup>

#### **Tool 2: Check Your Tech (Checklist Questions)**

The second tool provides signals of identified risk already being encountered and mitigated in the real world. For example, the signal provided for our sample risk zone, machine ethics and algorithmic biases, is Capital One pursuing "explainable artificial intelligence (AI)" to guard against bias in its models.<sup>10</sup>

The tool also provides a checklist of questions for each of the risk zones. For risk zone 4, these include:<sup>11</sup>

- Does this technology make use of deep data sets and machine learning (ML)? If so, are there gaps or historical biases in the data that might bias the technology?
- Have instances of personal or individual bias entering into a product's algorithms been observed? How could these have been prevented or mitigated?
- Is the technology reinforcing or amplifying existing bias?
- Who is responsible for developing the algorithm? Is there a lack of diversity in the people responsible for the design of the technology?
- How will an auditor push back against a blind preference for automation (the assumption that AI-based systems and decisions are correct and do not need to be verified or audited)?

## **“RELEVANT RISK ZONES AND THEIR RELATED QUESTIONS SHOULD BE SHARED ACROSS SYSTEMS DEVELOPMENT TEAMS.”**

- Are algorithms transparent to the people impacted by them? Is there any recourse for people who feel they have been incorrectly or unfairly assessed?

Relevant risk zones and their related questions should be shared across systems development teams. They should be kept front-of-mind when developing new products or considering new features. The most relevant questions should be added to product requirements documentation.

IT auditors should use these questions in audits to begin thinking how risk areas might be mitigated in the projects and/or applications under development in one's enterprise.

#### **Tool 3: Future-Proofing (Embedding Learnings)**

This tool is about embedding learnings from tools 1 and 2 and considering best practices for the future. This is done by suggesting a number of future-proofing strategies. For example, should all future technical hires complete a course or training in technical ethics before joining the enterprise? Should individuals take a data Hippocratic Oath as a condition of employment? Similar to technical vulnerability bug bounties, should an enterprise employ ethical bounty hunters? Should auditors prohibit irresponsible or unethical design, and counteract the prevailing "move fast, break things" culture of today's tech world?

I realize that many of these are lofty goals and would share the concerns of any IT auditor in recommending a required data Hippocratic Oath to one's chief information officer (CIO). Nonetheless, although ISACA is now past 50 years old, the information technology industry is a relatively young one when compared to, say, medicine or even accounting. I have no doubt that many of these concepts are the future. At a minimum, we, as IT auditors, should be aware of them now and should advocate for them where possible.

## **Conclusion**

In a previous column, I wrote about growing up in relative poverty,<sup>12</sup> a condition I shared with my

“ I BELIEVE THAT IF WE EACH BEHAVE ETHICALLY, WE CAN HELP MAKE A DIFFERENCE. ”

lifelong friend and ISACA colleague Martin Cullen.<sup>13</sup> I remember, as young seventeen-year-olds, discussing being unfairly treated due to bias (based on where we lived) when a song by Bruce Hornsby<sup>14</sup> came on the radio. The chorus of the song includes the lines “That’s just the way it is, some things will never change.” We both nodded our agreement and, at the time, our acceptance. In a world where data is the new oil, any such bias can be amplified and put to inappropriate uses<sup>15</sup> in information systems. Information systems, which, in many cases, we as IT auditors review.

However, the next line of the song’s chorus, which we conveniently ignored as we wallowed in self-pity, reads, “Ah, but don’t you believe them.” And I don’t. I do not accept that this is just the way it is. I believe that if we each behave ethically, we can help make a difference. Tools such as the Ethical OS can provide direction, aiding us in behaving more ethically in our work, which will, ultimately, have a positive impact on the reputation and, in turn, finances of our enterprises.

In addition, I am delighted to see ISACA launch its One In Tech<sup>16</sup> foundation. Among its primary goals are plans to engage in conversations about the social and ethical implications of technology and to grow and diversify the digital workforce.<sup>17</sup> We IT auditors can make a difference, however small. Volunteer now.

### Author’s Note

It would be inappropriate of me to sign off as the IS Audit Basics columnist without thanking you, the readers, for your support and many kind words. I have literally had correspondence from all over the world. Thank you.

I would like to thank my family and, especially, my wife, Geraldine, for the time and space to author this column. I will need to find a new excuse for not doing chores around the home.

I would also like to thank the staff at the *ISACA Journal* for their support over the last 3.5 years.

Finally, I would like to reserve a special thanks for the Managing Editor, Maurita Jasper. Believe it or not, we have never spoken, but we have, as you can imagine, traded many, many emails. Through this correspondence, I have come to know Maurita as someone who meets all of the ethical standards to which this article aspires. I am certain that the next *IS Audit Basics* columnist and, indeed, the *ISACA Journal* itself is safe in her hands.

### Endnotes

- 1 ISACA®, *ITAF: A Professional Practices Framework for IS Audit/Assurance*, 3<sup>rd</sup> Edition, USA, 2014, <https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf>
- 2 ISACA, *COBIT® 2019: Introduction and Methodology*, USA, 2018, <https://www.isaca.org/resources/cobit>
- 3 Ethical OS Toolkit, <https://ethicalos.org>
- 4 *Ibid.*
- 5 *Ibid.*
- 6 *Ibid.*
- 7 REX, [www.rexhomes.com](http://www.rexhomes.com)
- 8 Cooke, I.; “Developing the IT Audit Plan Using COBIT 2019,” *ISACA® Journal*, vol. 3, 2019, <https://www.isaca.org/archives>
- 9 Cooke, I.; “Audit Programs,” *ISACA Journal*, vol. 4, 2017, <https://www.isaca.org/archives>
- 10 Castellanos, S.; “Capital One Pursues ‘Explainable AI’ to Guard Against Bias in Models,” *The Wall Street Journal*, 6 December 2016, <https://blogs.wsj.com/cio/2016/12/06/capital-one-pursues-explainable-ai-to-guard-against-bias-in-models/>
- 11 *Op cit* Ethical OS Toolkit
- 12 Cooke, I.; “Add Value to What Is Valued,” *ISACA Journal*, vol. 4, 2018, <https://www.isaca.org/archives>
- 13 Martin Cullen is the certification director at the ISACA Ireland Chapter (Dublin, Ireland) and co-authored a column with me. Cooke, I.; M. Cullen; “Affect What Is Next Now,” *ISACA Journal*, vol. 6, 2018, <https://www.isaca.org/archives>
- 14 Hornsby, B.: *The Way It Is*, RCA Records, USA, 1986, [www.brucehornsby.com](http://www.brucehornsby.com). Bruce Hornsby is an American singer-songwriter.
- 15 Cooke, I.; “In Defense of Privacy by Design,” *ISACA Journal*, vol. 3 2020, <https://www.isaca.org/archives>
- 16 ISACA, One In Tech, <https://www.isaca.org/one-in-tech>
- 17 *Ibid.*