Implementing Emerging Technologies: Agile SDLC Still Works

It was a big deal scheduling network operation center (NOC) tours for customers when I was a client account director in network services, but the tours were always worth the extra effort. The center itself was impressive, with a walkthrough area that included hands-on telephony demonstrations, with coffee areas along the tour route for quiet conversation with lab engineers. The main show was the impressive command center, demonstrating not only how network traffic was monitored, but delving into how the network used predictive technology to anticipate traffic patterns and reroute voice, data, and video seamlessly and without human intervention.

A hallmark of the command center demonstrations was a review of several "catastrophic" events when the network rerouted traffic, not based on algorithmic anticipation, but by finding and taking advantage of the extra network capacity that was earmarked for disasters and network traffic surges alike. Unlike earthquakes or severe weather, human behavior is often predictable, and algorithms bordering on artificial intelligence (AI) "expected" peak traffic on the US Mother's Day holiday, and ebbs and flows for business behavior typical for a busy Monday or a quieter Friday. The network learned from itself, examining traffic patterns across the different data types and adjusted future routing with accuracy. Once such unexpected human event happened at the turn of the 21st century, catching the eyes of the command center and then the interest of the NOC tour guides: It was the extraordinary peak in network traffic that resulted from the first *American Idol* television show in the United States, where viewer voting caused earthquake-like volumes of network traffic. The graphs were displayed during client tours, showing dramatic changes in network flows—a memorable way to show the value of predictive routing.

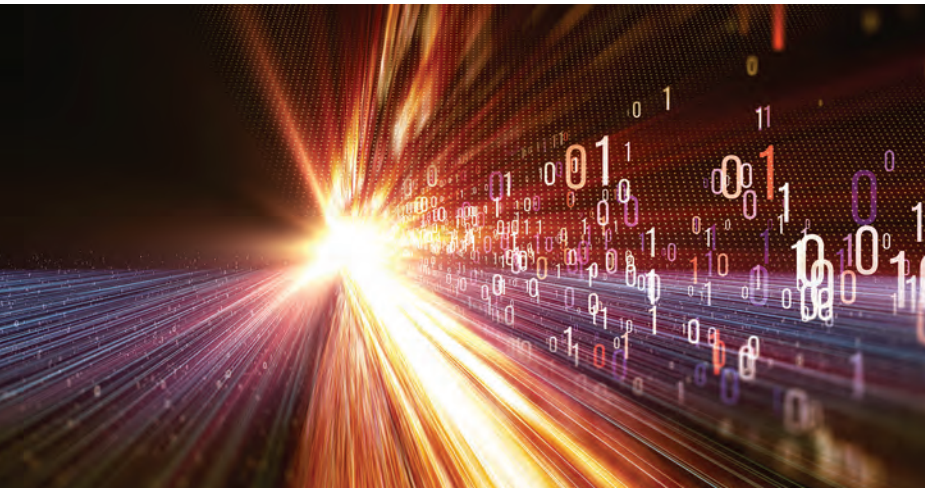
Seamless, predictive technology is a must-have for smooth communications and never caused public concern regarding how algorithms were used. The *ISACA® Journal* article, "Algorithms and Audit Basics" referenced the 1999 movie *The Matrix* that spurned a wariness of machine takeovers through AI;[1] but now, as we approach the quarter century-mark, AI appears in films such as *Ron's Gone Wrong*[2] and *Free Guy,*[3] where AI is part of everyday life, not just a necessity, but desirable. The advancements enabled by AI are inspiring, even at this relatively early stage. Yet inspiring innovation and increasing acceptance of AI do not reduce the worry many have. They call into question whether technologists worry about the right things when it comes to AI and, for us as a risk management and IS audit community, whether we are creating best practices to conduct the needed oversight for this emerging area. They also raise interesting questions regarding how to balance oversight with the needs of structured governance and a control framework in a manner that does not kill the innovation that is already around us.

Thoughtful Risk Management

Every technology carries risk, but the perceived loss of control inherent in emerging technologies such as AI compels users to feel a greater risk. And there are huge risk factors to consider, including:

CINDY BAXTER | CISA, ITIL FOUNDATION

Is director at What's the Risk, LLC. Her practice focuses on integrated risk control and process assessments for cybersecurity, privacy and business continuity/disaster recovery. She views risk management and control assessment as a chance to learn the nuts and bolts of a client's business and help them worry less, because gaps have been uncovered and a stronger operating model can be built. Baxter draws upon her experience in banking, insurance, healthcare and technology after holding compliance and management roles at State Street Corporation, American International Group (AIG), Johnson & Johnson and AT&T. When she is not doing risk and audit work, she enjoys volunteering on climate and environmental issues that impact her community.



- Privacy risk scenarios that carry consequences regarding insurability, identity theft and the risk of incarceration for uncommitted future crimes based on predictive profiling
- Data inaccuracy risk scenarios that lead to incorrect algorithmic outcomes, including driverless car accidents or incorrect medical research conclusions and potentially harmful treatments
- The risk of undue influence as marketers use persuasive selling by predicting potential product interest to transform buying behavior that is not beneficial to the consumer

Every technology carries risk, but the perceived loss of control inherent in emerging technologies such as AI compels users to feel a greater risk.

This short list is only a thumbnail of all the potential risk that AI brings, but locking the door and throwing away the AI key ignores the potential gains of the positives benefits, such as:

- Speed-to-market medical solutions that reduce wait time, save lives and provide a positive economic impact for otherwise overburdened healthcare systems
- Accelerated responses to emergency planning for meteorological events that previously cost many more lives than today
- Accurate analytics that solve criminal cases and protect the public
- Modeling capabilities that help future-solve climate issues and promote timely resilience

Technology has always sparked debate and concerns over social and economic justice, prompting evaluation regarding whether there is enough control over new and untried innovation. The concept of change alone, even without the added element of emerging technology prompts worries over lost employment, excessive oversight and privacy sacrifices. Risk analysis is fine, but when it comes to innovation, who is determining the risk, and is the perspective they represent fair? The present controversy over Clearview AI[4] lends credence to how challenging an appropriate risk assessment may be. When the field is crowded with potential inventors, the standard-bearers often produce detailed results that are difficult to interpret, as are the US National Institute of Standards and Technology (NIST) updates on *Facial Recognition Vendor Assessmen*t, the latest update of which is more than 400 pages long.[5]

While the Debate Goes on, SDLC and Change Control Still Matters

Thankfully, there are frameworks available to oversee and govern the great unknown that technical innovation represents. ITIL has morphed from v3 to v4 and addresses service operations structures from Agile and Waterfall to DevOps and Lean, but the core principle of consistent review of new and updated technology rests squarely on collaboration between developers, operations management and users in the business. The principle works to provide what users want via a jointly agreed-upon service catalog all the way through technology service go-live and post-deployment problem review, again with the user community present to determine and resolve flaws before full deployment. Does it really work in practice? With operations deadlines always looming and budget reductions that translate into software and system releases that do not include everything everyone expects, the project launch and change release processes are perfect intervention points for the IS auditor and compliance team. With AI at center stage in the media and top of mind for governments and organizations alike, the tried-and-true practices of change release and backup and recovery planning are perfect ways for IS audit professionals to keep technology, well, under control.

The Basics That Work

There are many articles on ITIL, Agile, Lean and DevOps. There are standards from NIST and frameworks such as COBIT®, in addition to the prescribed regulatory requirements. The concepts behind the software (and systems) development life cycle (SDLC) are as relevant as ever when it comes to encouraging technology advances in business, healthcare, the environment and more. What is SDLC and why is the framework so effective in making emerging technologies successful? SDLC is a structured approach to inspecting new development and new systems. It is also an excellent governance tool for managing upgrades to existing software and systems through its methodical framework.

The practical starting point is always the business case, where project and development ideas meet with approved funding. This early stage of project review has not been part of every audit or compliance job tour in the past, but more often, risk and control professionals are asking for and getting a seat at the table. Technology projects are reviewed for potential revenue generation, for technical/development feasibility and operational manageability. Determinations are made regarding buying the product/service from a vendor or building it in-house. This prestep to actual project launch is the optimal point of participation for risk management, where an inquisitive and objective technical mind can pose what-ifs and question operability and regulatory or enterprise compliance expectations. How often have projects launched that then get sidelined or passed into a long horizon of version upgrades to get to the original end goal? It is critical for risk and audit professionals to engage early and have a long memory regarding previous steps taken. Informed risk managers who provide critiques in early project stages, especially innovative technology such as AI, help mitigate the development rework that often happens on the way to meeting end user goals.

Risk management does not stop at the project funding and feasibility review phase of SDLC. Once finalized, the next major milestones compliance teams consider are development security validation and regulatory compliance verification, including sanctions checks. A governance checklist facilitates the reviews and provides documentation of both business and operations concurrence. What about Clearview AI's recent high marks for facial recognition accuracy from NIST? As risk, compliance and audit professionals know, there are no rubberstamp approvals when NIST completes a review. Although NIST provides valuable data to consider, software and system attributes must be applied and evaluated to the approved business use for the project, understanding the regulatory requirements and the inherent risk to the business regarding financial impact, regulatory impact, reputational impact and client impact. If this is not done at the project level, the risk of questionable interpretation might replace the conscientious and collaborative dialogue needed for project success and user satisfaction.

Informed risk managers who provide critiques in early project stages…help mitigate the development rework that often happens on the way to meeting end user goals.

Once the key compliance milestones of project acceptance, buy vs. build, and security and regulatory requirements have been completed, the development scrutiny starts. In-line inspection, whether it is a first line of defense review or internal audit interjected in a DevOps flow, using a combination of automated and manual control points keeps innovation going with less backtracking. Collaboration with business users is essential for crucial checkpoints in the development cycles regarding project intent, risk and expected outcomes. What should practitioners look for in the development testing phase? Several key checkpoints include:

- Review of the stated service/product to be provided to align with the project intent. This review, when done in-line, should produce the service delivery outcome expected of the project in a compliance way (compliance based on the governance checklist already performed plus agreement on key control points).
- Confirmation of business participation and documented approval as the steps proceed, story by story or phase by phase
- Evidence of key delivery milestones to confirm agreed upon dates, progress against those dates and impacts of any delays

LOOKING FOR MORE?

- Read *Destination: Agile Auditing. www.isaca.org/agile-auditing*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Reexamination of the key risk factors of reputation, customer and regulatory impacts are crucial to minimize unexpected or undesirable outcomes from innovation.

- Completeness and accuracy of test results with documentation fix plans for any failures, accompanied by business and operations approval
- Business acceptance of any changes—deletions, additions or modification to the service provided
- Evidence of infrastructure testing for capacity management of the new service/product
- Evidence of user acceptance testing (real users, not project/operational business reps) with authorized approvals attesting to the completed exercise and noting agreement to proceed

Important to successful deployment is scrutiny over change and release, where validation of the previous steps is reviewed and accepted by change management, verification of backout plan is done, and scheduling is determined in agreement with all parties and with sufficient developer and operations coverage in case of difficulties. The final steps of end user confirmation that everything is working as expected in production and post go-live business approval completes the flow with sufficient evidence that the outcome has met the expectations of all.

Innovative Technologies: A Bigger Deal Than Regular Project and Change Management

Emerging technologies such as AI are best managed post product/service deployment with timely monitoring controls that not only take the pulse of system and software effectiveness, but have control points that reexamine compliance with security, privacy and social justice requirements. Reexamination of the key risk factors of reputation, customer and regulatory impacts are crucial to minimize unexpected or undesirable outcomes from innovation, thus speeding adoption of the new technology.

Does the systems/software development life cycle and change release discipline provide the value and structure needed for emerging technologies such as AI without handcuffing innovation from moving into the mainstream? Can continuous monitoring by compliance and audit professionals get us to a new normal as portrayed in *Free Guy* and *Ron's Gone Wrong*? It can, but only when done in an inclusive, informed fashion where technologists, business partners, end users and those in the public are at the table conducting due diligence and control verification that looks toward continuous product/service improvement for everyone who may be impacted. More important, the due diligence team must have the ability and authority to halt questionable progress and require product/service modifications with the project team and business on board to fund and produce the needed updates.

Endnotes

1 Baxter, C.; "Algorithms and Audit Basics," *ISACA® Journal*, vol. 4, 2021, *https://www.isaca.org/archives*

2 Smith, Sarah, and Vine, Jean-Phillipe; *Ron's Gone Wrong*, Locksmith Animation, London, England, 2021

3 Levy, Shawn; *Free Guy*, 20th Century Studios, Los Angeles, California, USA, 2021

4 Hill, K.; "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, 10 January 2020, *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html*

5 National Institute of Standards and Technology (NIST), Face Recognition Vendor Test (FRVT) Ongoing, USA, *https://nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing*