THE Information Accountability Foundation
COLLABORATIVE POLICY INNOVATION

The Road to Expansive Impact Assessments – Why It Matters

June 2021

I. Introduction and Summary

Organisations will soon be conducting impact assessments that are much more expansive and rigorous than are required by today's data protection and privacy laws following where some leadership organisations have moved to. The driver of this trend will be the risks associated with Artificial Intelligence (AI) driven decisioning. These assessments will look beyond rights to seclusion and control to issues such as fair access to services and rights to meaningful employment. This approach may be driven first by organisations seeking to manage new, more complex risks associated with the use of AI but also on requirements relating to government procurement. However, it eventually will be mandated by new laws governing the use of AI and the associated fair implications to people.

The report of the Information Accountability Foundation (IAF) on Demonstrable Accountability - Why It Matters (Report) noted "Artificial Intelligence (AI) is beginning to affect almost every aspect of society. While harnessing its potential for good is an opportunity, addressing its risks will require an end-to-end comprehensive, programmatic, repeatable demonstratable governance system for adoption by all organisations seeking to use these complex systems as part of their strategy and objectives. The associated governance model, which includes broad, risk-based decision-making assessments, will be a step beyond the accountability required for less complex data processing and will require a "trust" driven approach rather than just a "legal" compliance approach to accountability. This approach evolves accountability based on legal requirements to accountability based on "fair processing" of data." In short, trust in more complex, more opaque systems that have impact on individuals will require more fair processing obligations on users of these systems, and these obligations must be demonstrable.

Since the release of the Report, further study has illuminated the key role impact assessments play in a demonstrable governance model. To understand this issue more completely, the IAF took a deeper look at some of the organisations studied in the Report. However, this study quickly evolved into the role the adoption of AI and the associated advanced governance model was going to play. By extension, the drivers of "responsible" AI indicate that the push for a different and more expansive governance model is likely to come from the AI community and not the data protection community. It also suggested this trend will be driven by several factors, only one of them relates to new laws. For example, public sector procurement is likely to create more immediate requirements on any organisation doing business with the government in key jurisdictions that will encompass these expansive requirements.

No matter the initial motivation, it is likely laws will follow. A prime example of this type of legal trajectory is the recently released EU Proposal for a Regulation laying down harmonized rules on artificial intelligence (Proposed Artificial Intelligence Act) with its myriad requirements on organisations. In the U.S., standalone AI related legislation and the requirement for more comprehensive assessments is part of some proposed Federal legislation and State enacted privacy legislation..

AI introduces new risks in terms of not just the impact on stakeholders but in the way this technology, and the data that enables it, is developed, and deployed. AI is different from traditional software requiring new governance procedures. For example, the data used to build models needs to be analyzed for many contributing impacts, such as the inherent bias found in many data sets. The deployment of the resulting model which may have additional risks, such as bias and discrimination properties, also requires assessment. The result is not only a new set of procedural requirements to address these risks that need to be designed and implemented by organisations, but the resulting impact assessment becomes a self-repeating analysis of not just the end impact of deployment, but the impact of how

particular development requirements were applied. This outcome means organisations will have to develop skills and resources to both design and implement the governance requirements and then assess each AI application so that it maximizes benefits and mitigates risks appropriately.

While AI will require more expansive assessments, regulators today are observing a lack of risk assessment capabilities in organisations required by current laws. These new requirements will require new skills and capabilities in organisations. It also means new skills and resources will be required by regulators, especially as laws and associated enforcement models get developed.

To enable trust-based AI that is demonstrably fair, organisations and regulators will need to evolve. This report on the role of expansive impact assessments first takes a deeper look at some of the original organisations studied as well as a view of demonstrable accountability by data protection regulators. It then goes on to outline the role assessments play and to analyze the drivers of more complex assessments such as Algorithmic or AI impact assessments (AIA) and then concludes with a deeper look at the role of AI and its associated governance needs as a driver of this trend.

I. From the Perspective of the Organisation's Studied

A. What are Leading Organisations Doing with Assessments?

In the Report, IAF profiled what twelve leading companies are doing to build trust in data innovations through enhanced accountability, while at the same time noting there is an accelerating trust gap between some regulators and general business practices. Driving this trust gap, regulators have expressed disappointment at how unprepared some organisations are to meet even legal compliance driven requirements, such as Data Protection Impact Assessment (DPIA) risk assessments, let alone demonstrating the type of risk-based decision making required for more complex technology and data use scenarios.

These leading organisations are going beyond compliance to drive for broader business objectives:

- **Digital trust (not regulatory compliance) is the strategic driver**, and this development is being driven by tone at the top. Advanced data use is necessary to meet corporate objectives, and that use is dependent on public confidence that data is used in a trustworthy manner. This approach is driving investments well beyond meeting legal compliance obligations and aligning overall business strategy and (privacy) structures and programs in new ways.
- **Broadening the areas of focus of the Privacy Group** – To drive a business objective that requires trusted technology and trusted data, functions such as data ethics, end to end data governance and, most significantly, AI governance are being added to the group privacy office remit. Collaboration is increased significantly with other key functions such as advanced analytics teams, data governance teams, and operational risk functions. These functional groups are also becoming more intertwined.
- **Review processes (Privacy Impact Assessment (PIA)/DPIA/Ethical Data Impact Assessment (EDIA)) are significantly broadening** and are focused now on customer and user impact and trust and organisational reputation. In some organisations, a standard PIA is no longer used. A much broader "impact" assessment has taken its place addressing broader risks to people.

- **Risk based, formalized escalation processes are being established** - Different levels of formalized senior leadership involvement is becoming the norm for impact reviews of new/revised products and services.
- **Instrumentation and formalization of digital organisation wide accountability** - Even in heavily culturally driven organisations, there is a shift to "organising the culture."

A key part of their investment scope and a key element of Fair Processing Accountability is in the areas of assessments and risk centered decision making.

B. Recap of Key Findings on Assessments

A key investment these leadership companies have made is in the area of project or product assessments. Given the role assessments and decision-making processes will play in demonstrable fair processing, IAF looked deeper in the investments TELUS, Sun Life, IPG Media Brands, Acxiom and Facebook are making.

As noted in the Report, at these leading companies, review processes such as PIAs or DPIAs are being expanded to include a broader set of elements**.** AI governance, ethics, algorithmic model evaluation, end-to-end data analysis, including all types of data, and fairness are elements that are being added. The evaluations are aligned with the company's strategy and digital trust objectives and are becoming more like an Ethical Data Impact Assessment (EDIA) as what was proposed in the IAFs work with the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD). They are evolving further into models that are being contemplated in many of the proposals related to AIAs. In short, these organisations have taken a base privacy impact assessment or even a DPIA as required under the European Union's General Data Protection Regulation (GDPR) in certain higher risk data scenarios and broadened them in two significant ways.

First, they have added questions in their assessment process that go well beyond what would be found in a typical PIA or DPIA. These touch on fairness, discrimination, and increasingly algorithmic development and deployment. They start with the premise that ALL data, not just personal data, are in scope and use an initial threshold type process that determines the level of rigor of the subsequent questions of the assessment process. This approach weeds out/facilitates a lighter weight assessment for scenarios that have little to no risk (e.g., non-personal data used for a business operational objective). They have requirements embedded that even if non-personal data are being used, if the data start to impact an individual, the assessment process requires the project team to reevaluate. Typically, any new data or data source or any new use of data trigger the need for an assessment. Assessment processes are iterative and involve checkpoints along the project life cycle.

All companies have clearly defined, multiple escalation processes for higher risk/impact projects and use some form of risk tiering methodology to determine escalation and approval levels. As part of the multi-tier review process, there are many defined points where there is a second line of defense involvement. Some companies have a compartmentalized assessment process separating out knowledge discovery, for example, development of insights, from application of knowledge or insights from "sandbox" environments. One organisation is experimenting with Risk Foresight Workshops analogous to Threat Modeling tabletop exercises in security processes and/or Microsoft's "jury" process in its Responsible AI process.

Second, they have deliberately created assessment processes that are not only integrated into the project or product development lifecycle but are engaging all parts of the lifecycle in assessing risks. They all are at some stage of **"**tooling" both the process and culture to "technifyng" or systematizing accountability. This involves tighter integration with existing business development processes but also ties to technology and process that are more integrated with parts of enterprise data management. Companies are either significantly updating/investing in their own tooling or substantially modifying other tools/platforms they may use. They are adding or formalizing technology aided escalation points. During the life cycle of a data element, a number of companies are adding decision outcomes to that data element (i.e., data tagging) to achieve agreed to parameters with respect to data or its use. As two of the organisations put it, "the accountability and ability to ensure commitments are met is not possible absent top to bottom, technology enabled accountability; technifyng the culture of accountability."

Structurally, these added governance responsibilities in the organisations studied have been added to the Group Privacy Office. An alternative structure is emerging in some companies, for example Microsoft, where the Office of the Chief Responsible AI Officer has assumed the development and implementation aspects of AI governance, distinct from the Group Privacy Office.

To gauge where demonstrable, fair processing accountability is going, or needs to go, the view of the Regulator is key.

II. From the Regulators' Perspective

A. What do Regulators View or Expect as part of Demonstrable Accountability?

It is the view of the IAF that advanced accountability requires active demonstrability for processes to be trusted by regulators. Such active demonstrability might include, for example, greater transparency by organisations as to their use of data and the decision-making processes they employ. However, the current laws and associated regulatory attitude do not require this approach. Instead, demonstrability, today is at the request of the regulator. For example, "*being able to demonstrate,*" as called for in Article 5 of the GDPR or accountability guidance issued in Canada and Hong Kong, remains an "on demand" approach as opposed to a more proactive requirement.

A key measurement by regulators in being able to demonstrate a program's capabilities is the organisation's demonstrated ability to effectively assess the risks data processing creates. In Europe, the DPIA process is paramount, including the capability of being able to demonstrate top to bottom organisational identification of risks and mitigations plus the associated records of processing. A DPIA is a useful proxy as it requires the assessment of a full range of interests of a data subject, and at least in the viewpoint of one Regulator, is where Recital 4 of the GDPR is important. Specifically, Recital 4 states: "The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality." This viewpoint is more in keeping with what the leading organisations studied have embedded into their assessment process. However, it is key to note the assessment of a "full range" of rights and interests has not yet evolved for most organisations and is currently, for the most part, more narrowly looked at relative to privacy and data protection by most regulators. As such,

the evolution of assessments more akin to fair processing accountability, is unlikely to mature through data protection or privacy enforcement.

As highlighted in many conversations with data protection regulators, to date, "it is unusual to see a good assessment process that fully identifies risks appropriately." While, in Europe this view brings into question the effectiveness of DPIAs and by extension, legitimate interest assessments, in other parts of the world, it brings into question the effectiveness of organisations' overall privacy programs. This result in no small part contributes to a lack of trust some regulators have indicated with respect to the commitment of business to meeting accountability requirements, even today. As highlighted in the Report, there is a marked difference between many organisations and their level of program-investment. and the leading organisations studied. This difference also highlights a tension recognized by Regulators; achieving the type of "balancing" a DPIA risk culture implies (e.g., a multi-stakeholder "risk" analysis) requires a pivot beyond a strict (minimalistic or limiting) regulatory compliance only approach.

In Europe, the evolution of demonstrable accountability likely will develop through Codes of Conduct (CoC) and the accompanying certification/attestation process as part of implementing Article 40 of the GDPR. The assessment process of the organisation's part of the CoC will be key, and as already signaled by regulators, many CoC's will require a third-party attestation process. There is built in confidence In Europe as to the "certifiers." For example, in the UK and Ireland, certifiers have to be approved according to National Standards (Certification of the Certifier). In France, the CNIL plays a role in approving certifiers.

In Singapore, the trust mark program and process are viewed to be the vehicles where additional requirements of organisations, due to the use of advanced technologies such as AI, will be introduced and attested to. There is a high degree of transparency with the Trustmark process.

One regulator believes a trend of CoCs will involve some form of public view of the assessment process; this aligns with the IAF recommendation relative to transparency of processes as noted in the People Beneficial Data Activities work done in Canada. Some organisations such as TELUS, Mastercard and of late Facebook have started to more proactively communicate their practices and intent; however, these examples are few.

Related to increased transparency and more visibility, In Europe, under Article 35(9) of the GDPR , a controller must seek the view of data subjects on the processing subject to the DPIA. A proxy could be an ethical advisory function or civil society input, which some organisations are starting to use.

Considering the limitations of DPIA's (see below), and specifically what rights and interests they cover, as well as the narrower evolution of existing data protection laws in other regimes, the evolution of expansive impact assessments and risk-based decision models is likely to come from other areas and be driven by AI adoption.

III. The Role of Assessments

A. What Roles Do Assessments Play in Trusted Fair Processing?

In much of the IAFs early work on Big Data, Ethical AI, and Data Stewardship and even Legitimate Interests and Integrated Risk and Benefits, an "assessment" has been a core element. In most of this work, the core premise has been "an [assessment] is a process that looks at the full range of rights and interests of all parties in a data processing activity to achieve an outcome when advanced data analytics may impact people in a significant manner and/or when data enabled decisions are being made without the intervention of people. An [assessment] assists an organisation in looking at the rights and interests impacted by the data collection, use and disclosure in data-driven activities." While clearly the focus has been on the need to assess the impact of data use on all stakeholders who might be impacted and against a set of issues (risk and benefits) broader than just privacy, there are equally important elements of an assessment that help it serve as a key plank in effective governance.

First, it serves as a documentation of a data activity or project. This is key to meet GDPR requirements relative to records of data processing and basic, core sound governance. Second, it is a decision-making mechanism to help an organisation make complex decisions on whether benefits and risks (impacts) have been both balanced and optimized (appropriately mitigated in terms of risks). It not only aids the decision-making process by facilitating the analysis but serves as a record of the decision and a means to enable subsequent follow-up as part of agreed to controls that may apply to a particular project. Third, and related, it enables organisations to build and adapt over time; what worked and was sufficient for an assessment in 2021 may not be enough in 2024. But the fourth element is perhaps as important as the impact analysis portion; it is a memorialization as to how control requirements that have been set by the organisation have been applied in a specific technology and data scenario. What does this mean?

In many organisations, external requirements, such as laws and regulations, along with internal commitments, for example standards or even industry or company goals, are usually translated into a set of policies and procedures that guide the organisation's practices. Meeting these policies and procedures is often assessed and facilitated through a project assessment process.

A simple example is a PIA where specific legal requirements such as consent and transparency are translated into language (policy or procedure) that tells an engineer or marketer what to do and then a PIA assesses whether these standards have been sufficiently met. As the areas of potential impact get bigger and broader with advanced analytics and AI, the need to establish new policies and procedures that tell multiple roles what to do becomes more important. A key part of a well-constructed impact assessment determines how have these requirements been met and by extension how the impact objectives (maximize benefits and minimize risks) have been achieved. This process increasingly becomes important in AI situations. For example, working backwards, a potential impact might be a group of people who have been subject to inappropriate bias or even discrimination that may trace back to the inherent bias of the data used to develop and train the original AI model.

B. Drivers of Broader Assessments leading to AIA Models

There are a number of trends that will likely drive the adoption of more expansive assessments. "Expansive" means the assessment of both the scope of impact **and** the scope of requirements to meet impact objectives. This trend increasingly will encompass not just the impact of the use of data but also the use of the inherent technology itself.

1. **Competition** - As with the leadership companies that have implemented more advanced accountability processes, **organisational growth in the use of data and technology to achieve business objectives** and the parallel recognition of the added risks such use can create will result in more risk management tools like broader assessments being adopted. This risk recognition will include the dependency on "trust" in how organisations are using both data and technology. The tension on trust will come from a general perceived level of market trust whether it is driven by regulators, consumers, advocates, academicians, employees, or shareholders. This "beyond core legal compliance" approach will result in the adoption of governance processes to meet broader business objectives. The leadership companies will have followers.
2. **Growth in "reticence risk"** will ultimately morph into broader governance processes that will include more advanced assessments. In short, the organisational growth in the use of data and technology, absent effective governance, and decision-making tools ("should I do this"), will create tension between the business and the risk sides of the organisation. The result will affect decisions on whether to proceed and cause delays in or avoidance of certain activities, with the resulting sub-optimizing of value creation. Ultimately, the drivers of value creation will result in the adoption of broader and deeper governance processes that will include wide-ranging impact assessments as a means to streamline risk-based decision making.
3. Even before laws and regulations which will drive the need for expansive impact **assessments, Public Sector influence will have an earlier impact.** For example, in Australia, Canada, Singapore and shortly Hong Kong, governments have or will be implementing processes and requirements for their public sectors to address ethical and other risk challenges of AI. These guidelines often include AIAs. These internal requirements are likely to evolve to requirements on any government procurement activity, meaning any business wishing to sell or provide service to the government will have to meet similar governance requirements and be able to attest to these processes and procedures that will include AIA type assessments. This trend has already played out in the security space with requirements such as FEDMA (Federation of European Data and Marketing) in Europe or FISMA (Federal Information Security Management Act) in the U.S. and in many other countries globally.
4. While laws and regulations are likely to be enacted relative to AI that will include requirements such as AIAs, in the short term, even **regulatory guidance issued by DPAs,** and others will have an impact on organisational processes. An example of this is AI guidance issued by the UK ICO,[1] which requires a very different sort of internal assessment than even found in even complex DPIA's. However, public policy driven by government sponsored or supported initiatives is likely to create a class of "soft law" that will drive organisational governance activities like broader assessments. For example, as outlined in How do we ensure the responsible use of AI by Governments? - Digital Tech ITP,

[1] Guidance on AI and data protection | ICO, AI Auditing Framework | ICO, Explaining decisions made with AI | ICO

PWC's Maria Axente provides a UK example about the relationship between academia, public policy, regulation and/or soft law to develop ultimately organisational governance requirements.

5. **Specific Laws** - There are already many AI specific proposed bills in the U.S. and globally, and much governmental debate and investigation as to what should govern the impact (risks) of AI. These universally contemplate some form of impact assessment. Several proposed laws in the U.S. introduce specific requirements related to algorithmic assessments or risk assessments related to "automated decisions" which is becoming the proxy integration medium between AI and privacy. The growth in the use of AI likely will accelerate this trend. In terms of specific assessment type requirements, specific proposed laws include the Algorithmic Accountability Act and Algorithmic Fairness Act (U.S. Senate). What is also being seen is proposed privacy laws that either explicitly or implicitly require much broader type risk assessments than a PIA. For example, the Mind Your Own Business Act (U.S. Senate), Consumer Online Privacy Rights Act (U.S. Senate), and the Automated Decision Systems Accountability Act of 2020 (U.S. - California), as well as the Washington State and Virginia privacy bills which have similar assessment requirements. The EU's Regulatory Approach to AI contains specific risk assessment requirements, and while it does not explicitly require an AIA type assessment, it implicitly does. While privacy legislation is complicated enough, without packing in all the social and political issues that can arise from uses of information, recent privacy legislation introduced, such as the Mind Your Own Business Act, potentially pave the way for specific assessment type legislation. One possibility is the adoption of narrower, stand-alone privacy legislation covering algorithmic issues and the need for expansive risk assessments.
6. Related to and/or driving these factors is **the growth in the adoption of AI.** The growing appreciation of the broader range of risks and associated ethical impacts the corresponding AI assessment needs to address must be factored in as well. As Protecting privacy in an AI-driven world (brookings.edu) highlights, AI adds a level of complexity to an already complex privacy legislative environment. However, this adoption also increases the internal governance requirements of organisations using this type of technology and by extension the design of impact assessments.

C. The Driver of AI Adoption as a Driver of AIA type Assessments and Governance

While these trends are related and inter-related, they all tie to the impact of more complex analytical driven use of data used in AI. By extension, it is useful to look at the overall trajectory of AI usage and associated governance that includes broader impact assessments.[2]

[2]AI content was partly developed based on PWC's approach to Responsible AI and Six stage gates to a successful AI governance | by AnandSRao | Towards Data Science

To date there has been much more literature on the risks of AI, the need for ethical principles and the need for governance processes that include AI impact assessments [3] coming from academia, government and even business than what is seen in the data protection world. There are three main drivers of this:

1. The adoption of AI as part of organisational growth (both private and public sector).
2. The recognition of the risks associated with AI and the need to address ethical issues, and
3. The recognition AI requires a different sort of end-to-end governance and a different way of assessing the impact to people.

In terms of adoption, AI use is rapidly expanding within organisations, in both commercial and public sectors as a result of productivity gains and increased consumer demand driven by AI-enhanced products and services. It is used to automate existing processes, augment decision making, and to enhance customer experiences with new products and services.

In terms of risk recognition, unintended consequences can yield risks and potentially harms for both consumers and the organisations using and deploying AI and algorithmic decisions. Some of these unintended consequences are manifested as bias in applications from medical devices to entrance exams. According to a PWC AI Predictions Global Survey, the awareness of managing the risks of AI is increasing. "Companies are aware of them. The bad news? Most are not actually mitigating them."

As more companies rely on AI for critical decisions, AI risks increase. There are increasing calls for AI governance, including the adoption of AIAs to assess the potential benefits and risks, and risk remediation processes. By extension, organisations need to adopt and prepare for additional governance requirements, manage the risks of AI, and satisfy increasing demand by regulators, consumers, shareholders, and other stakeholders for accountability.

Accountability based governance increases with AI, given the complexity of the AI systems themselves. In addition to the opacity associated with these systems, there are differences between the development lifecycles of traditional software vs data science and AI. For example, "traditional programming relies online-by-line instructions for a computer to process the input data to produce the desired output that matches a given software specification. Conversely, data science, involves the input data and in some cases a sample of the output data to build a model that can recognize the patterns in the input data. Unlike traditional programming, data science models are trained by providing input data (or input and output data) to recognize patterns or make inferences. When fully trained, validated, and tested, they perform predictions or inferences on new data." There is a clear development stage of AI where models are built and tested that is distinct from a deployment stage. This introduces iterative

[3] AI Now: https://ainowinstitute.org/aiareport2018.pdf, CA:https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html, EU: https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment. From Andrew Selbst: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2819182, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3456224, Smart Dubai: https://www.smartdubai.ae/self-assessment, Governing with Algorithmic Impact Assessments: Six Observations by Emanuel Moss, Elizabeth Anne Watkins, Jacob Metcalf, Madeleine Clare Elish :: SSRN

analysis requirements and additive governance requirements related to model management and testing.

While calls for a new assessment such as AIAs are increasingly gaining momentum, proposed approaches rarely consider the relationship or potential overlap with DPIAs. Nor do they propose an effective methodology to assess the balancing of benefits and risks.

The AIA and DPIA are both risk assessment tools and partly use the same logic. Both instruments are complementary in terms of meeting regulatory requirements but are not interchangeable. To date, only the DPIA and PIAs are mandated, though it is becoming increasingly likely that regulations requiring AIAs will be created. For example, the EU draft AI Regulation requires "Conformity Assessments" for high-risk AI, and logically assessments will be required to determine if AI processing is high risk as well as whether other requirements proposed in the EU Draft AI Regulation have been met by a particular AI application.

However, even DPIA's are insufficient in the AI context. For example, DPIAs focus on the individual as opposed to a broader set of stakeholders, and even then, only as the technology involves the use of personal data. As noted in the IAF blog Transparency Needs a Makeover, terms in AI such as transparency and accuracy, have a much broader use and impact than in traditional data protection lingua franca. Even an effectively designed DPIA falls short in enabling an organisation to balance all interests across stakeholders and evaluate the ethical impact of AI and associated data use.

There is significant interest around AI governance improvements. For example, tech-oriented solutions to improve the traceability and lineage of models and data and AI/ML platform companies and the open-source community to solve for issues around bias and ethics are now available. While this is a promising development, effective AI governance cannot be a purely technology-led effort as it only solves for concerns technical stakeholders may have; it does nothing to assuage concerns posed by consumers, regulators, and requirements for end-to end governance that integrates with second and third lines of defense.

The Three Lines of Defense are a well-established concept in many organisations; even institutions that do not formally adhere to the construct of the Three Lines of Defense have similar functions: builders/creators, management, and compliance and internal audit.[4]

The Three Lines of Defense model provides a simple and effective way to enhance communication on risk management and control by clarifying essential roles and responsibilities. However, it exposes several potential needs in terms of addressing capability and competency gaps across each line:

- The development and deployment of AI requires technical competency and the right set of tools (e.g., fairness and bias testing). Assessment of skills and resources related to these needs should be performed across all first line roles with a plan to address deficiencies.
- Oversight is required to apply first line requirements effectively. This oversight could be performed by separate roles within the first line or by designated second line roles; increased capacity and capability will be required.
- Many first line requirements are codified in practice through standards or operating procedures, often established by second line teams. The creation of these procedures may require adding new

[4] See Three Lines of Defense - ERMA | Enterprise Risk Management Academy (erm-academy.org)

resources with newly required skills to second line teams.

- Third line functions often rely on established controls. Absent accepted standards, functions like Internal Audit will have to develop an initial set of controls to assess against. A partnership between all three lines should iteratively develop and assess control effectiveness.
- Increasingly more complex or risky AI will benefit from independent perspectives; some organisations are using data or ethical review committees to advise on these perspectives. Developing the right mix of process and committee member skill is required.

Unlike more of a compliance or even technical assessment, an AIA requires an iterative approach and review. For example, the impact may not be fully known at even the development stage of AI, and the approach to testing may not be fully evaluated for efficacy until the deployment stage is reached.

Also, self-reinforcing governance processes are necessary; many questions will require standards (policies) and operating procedures to be established as part of an end-to-end governance model, and each AI application will require both an appropriate and effectiveness evaluation against each of these standards. The flip side is the establishment of these standards and procedures will be key to informing different organisational roles as to what to do as they develop AI solutions requiring a different or expanded way that the three lines of defense may operate. It is clear new skills and capabilities will need to be developed and added to organisational roles and structures.

IV. Conclusion

Expansive AIA type assessments and decision-making will be required so that complex, data analytics systems such as AI are viewed as trusted and able to demonstrate Fair Processing Accountability. The drivers of these assessments and associated governance will come from multiple sources.

One driver will be public policy. However, given the complexities and tensions of evolving privacy legislation, public policy in the AI space is likely to have a larger impact. For example, with its announcement on 21 April 2021, the EU Commission has proposed an entirely new body of law, which intends to place ethical issues such as bias mitigation, algorithmic transparency, and human oversight of automated machines on a regulatory footing. Having said this, given the anticipated pace of regulation and legislation, drivers of this form of governance are more likely to come from elsewhere in the short term.

One implication is clear. While the type of assessment and governance requirements are still in flux, organisations will require additional investments to be made. These will include upskilling key roles in terms of their competencies (technical and behavioral).

While much focus has been given to the specific public policy and resulting governance requirements space, it remains unclear what form of enforcement and oversight is best suited to trusted fair processing. Regardless of how this space evolves, it is clear regulators will also need to upskill their competencies and make other investments.

The appropriate structure and mix of regulation and enforcement will require considerably more thought and further work. However, for all the trends noted, organisations should be developing these more complex governance systems. These systems include more expansive impact assessments, to enable their business strategies that increasingly will involve more complex technology and data use, to

meet growing market expectations related to fairness and to inoculate themselves from the likely direction of regulatory requirements.
