**Data protection impact assessments: a meta-regulatory approach**

**Reuben Binns**


Published:

28 April 2017
DATA PROTECTION IMPACT ASSESSMENTS:
A META-REGULATORY APPROACH

Article category: Original Article

Summary:

- Privacy and Data Protection Impact Assessments (PIAs / DPIAs) are tools for organisations to manage privacy risks. They emerged in various jurisdictions from the 1980s, initially as a purely voluntary measure. DPIAs are now set to become a mandatory requirement in certain circumstances under the European General Data Protection Regulation (GDPR). This article addresses impact assessments from the perspective of regulatory theory. Their transition from a voluntary tool to a mandatory requirement raises questions about their purpose and role, as well as implications for the direction of data protection in Europe more generally.

- Previous analyses have tended to assess such impact assessments in relation to a limited set of regulatory categories, namely self-regulation, command-and-control regulation, or some form of 'co-regulation'. Drawing from regulatory theory, this article suggests a more nuanced account of the mandatory impact assessment regime outlined in the GDPR.

- It argues that this regime can be understood as a form of 'meta-regulation'. The final section draws on a framework for assessing the prospects of meta-regulation, in order to assess the prospects for a meta-regulatory approach to impact assessments.

Keywords: Data Protection, EU, GDPR, Impact Assessment, Privacy, Regulation

1. Introduction

A PIA is a process of assessing the possible privacy implications of new uses of personal data. Proponents of PIAs argue that they could be a promising solution to address privacy and data protection concerns. PIAs are designed to help organisations implement 'privacy by design', by incorporating privacy considerations into their activities and projects from the early stages, thus reducing the risk of privacy violations and any associated regulatory action or reputational damage. As the following sections describe, PIAs have evolved from a tool used by some organisations voluntarily, into various internationally recognised and increasingly mandated practices. PIAs have been lauded as 'the most comprehensive tool yet available for policy-makers to evaluate new personal data information technologies before they are introduced', capable of imagining the 'unknown unknowns'. However, alongside these bold claims, there is also significant ambiguity around what exactly constitutes a PIA, and different terms – such as ‘Data Protection Impact Assessment’ – have been coined to denote related but substantively different tools and requirements.

Given the ascendant enthusiasm for impact assessments and the perceived risks of data processing, it is not surprising that their use is increasingly urged by regulators. This has culminated in the inclusion of new provisions in the European Union's proposed General Data Protection Regulation (GDPR). Article 35 of the GDPR requires organisations to conduct impact assessments prior to types of processing of personal data which are likely to ‘result in a high risk to the rights and freedoms of natural persons’.

---

6 Wright & P. De Hert (Eds.), Privacy Impact Assessment (pp. v–xiv). Springer.
10 European Commission. (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 0011.
A great deal has been written by academics and practitioners about the ideal form of such impact assessments. However, debates about their merits and purpose have generally not drawn significantly from the large body of regulatory theory. This article aims to fill this gap. In particular, it is argued that in making impact assessments a regulatory requirement, the GDPR has transformed them from a tool of self-regulation into one of 'meta-regulation'.

The notion of meta-regulation, introduced by Christine Parker, describes state efforts to make corporations responsible and accountable for their own efforts to self-regulate: i.e. 'legal meta-regulation of internal corporate self-regulation'. A purported advantage of meta-regulation over other forms of regulation is that it latches onto companies' inherent capacity to manage themselves, but without letting them off the hook if their self-regulation efforts fall short of regulator (and stakeholder) expectations. It aims to leverage corporations’ existing management structures and internal bureaucratic processes in the pursuit of regulatory goals. Companies may be forced to evaluate and report on their own self-regulation strategies so that regulatory agencies can determine whether the ultimate substantive objectives are being met. Examples include occupational safety or food regulations which require firms to engage in their own processes of hazard identification, risk assessment and risk control. I argue that this approach, if undertaken appropriately, has the potential to address some of the key challenges identified by the Commission in their motivation for data protection reform.

---

11 Ibid., 8.
12 Ibid., 5.
14 Ibid, p. 8
15 Ibid, p. 13
17 Ibid., 98, p. 27
2. Privacy Impact Assessments: Background

This section provides some background on PIAs relevant to the discussion in subsequent sections.

2.1 Origin of PIAs

PIAs could be seen as an evolution of provisions set out in early data protection regimes in which organisations were required to register, notify and check with national authorities to ensure compliance prior to processing.\(^\text{18}\) However, advocates of PIAs have argued that they go beyond mere compliance checking, citing a need for a wide-ranging, contextually sensitive and 'holistic' approach.\(^\text{19}\) According to a history of PIAs produced by Roger Clarke, the concept of a PIA is derived from instruments in other policy areas like environmental law, which allow for this broader perspective.\(^\text{20}\) They became established as a concept in policy circles in the late 1990's, primarily in English-speaking common law countries, particularly Canada, Australia and New Zealand.\(^\text{21}\)

By 2000, PIAs were regarded by a subset of Privacy Commissioners, consultants, data protection professionals and academics as an 'essential tool for data protection'.\(^\text{22}\) There was

---

\(^{18}\) The European Data Protection Directive of 1995 institutionalised 'prior checking' and notification with a national authority (Article 20), but similar provisions are contained in data protection acts pre-dating the 1980 OECD Guidelines, e.g. Sweden (1973), Austria, Denmark, France and Norway (1978). Prior checking has been characterised as a 'forerunner' to PIAs in Le Grand, G., & Barrau, E. (2012). Prior Checking, A Forerunner to Privacy Impact Assessments. Ibid., 8 (pp. 97–115).


\(^{20}\) Ibid., 1.

\(^{21}\) Ibid., 1, p. 126

also growing interest from the private sector at this time, partly due to the perceived challenges facing multinational organisations in cross-border compliance.\textsuperscript{23} By the mid 2000's, a number of national privacy and data protection authorities, government departments, and regulators had begun producing guidance on conducting PIAs.\textsuperscript{24} These guidance documents indicate that policy-makers had converged on a set of core features of PIAs. They stress that a PIA is not just a tool or a report, but a process. The subject matter of a PIA is a 'project' (which encompasses any 'system, database, program, application, service or scheme, and enhancement of any of these, or an initiative, proposal or a review, or even draft legislation'\textsuperscript{25}), and its impact on privacy. They are distinguished from activities with a narrower scope, such as privacy audits, because they begin \textit{before} rather than \textit{after} implementation.\textsuperscript{26} Nor are they synonymous with legal compliance assessments, because they deal with 'qualitative matters of legitimacy, participation and proportionality' rather than just compliance with specific rules.\textsuperscript{27} They are for 'organisations of all sizes' and can be performed in-house or by external consultants.\textsuperscript{28} While these guidance documents often include accompanying templates, organisations are cautioned against seeing the PIA process in terms of a one-size-fits-all solution.\textsuperscript{29} More recently, the Privacy Impact Assessment Framework Consortium (PIAF), an EU-funded PIA advocacy group, has defined a PIA as:

\begin{quote}
\textit{a methodology for assessing the impacts on privacy of a project, policy, programme, service,}
\end{quote}

\begin{footnotesize}
\begin{enumerate}
\item The PIA guidance produced by national authorities in Australia, the UK and Canada are regarded by some as the 'most comprehensive and practical guidance documents available in any jurisdiction' (Clarke, R. (2011). An Evaluation of Privacy Impact Assessment Guidance Documents. International Data Privacy Law, 1(2), 111–120.). European countries with PIA guidance include Slovenia, Spain, Germany and the UK. Other privacy / data protection authorities with guidance documents include Hong Kong, New Zealand, Canada, and the US (multiple government departments).
\item The ICO defines privacy audits as “the detailed analysis of systems that are already in place against a prevailing legal, management or technology standard” (Information Commissioner’s Office. (2014). Conducting privacy impact assessments code of practice.)
\item Ibid., 25.
\end{enumerate}
\end{footnotesize}
According to their proponents, a primary aim of PIAs is to manage risks associated with threats or vulnerabilities arising from processing personal data. They should therefore be integrated with risk management processes (but are not synonymous with them). As well as impacts on individuals, they should consider direct and indirect impacts on the organisation (e.g. fines and penalties, opportunity costs or damage to brand reputation). The process of a PIA should be documented in a report, which should include a description of the assessment, as well as terms of reference, deliverables, and responsibilities. The purported benefits for organisations who conduct PIAs include greater transparency and trust, confidence, valuable stakeholder input, understanding and respect, avoiding liabilities and crises down the line, and identifying cost effective solutions.

### 2.2 Adoption and implementation of PIAs

In certain jurisdictions, public bodies are required to produce a kind of PIA (although, as I discuss later, this activity may not be considered a ‘real’ PIA). Private organisations have so far undertaken PIAs at their own discretion. The precise extent of PIA activity in either sector is not clear, because much of it goes unreported and a relatively small number of PIAs are published openly. Various sector-specific PIA initiatives are underway or have been proposed, and an ISO standard involving PIAs is in progress.

European interest in PIAs was arguably precipitated by the 2007 PIA handbook, published by

---

31 ‘Determining the risk(s) resulting from various vulnerabilities and threats requires some analysis and assessment, which is what a PIA can and should do.’ (ibid., 8., p9)
32 Ibid., 8, p15
34 See ISO 27001 (http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)
the UK Information Commissioner's Office, and the European Commission's recommendation of PIAs for RFID (Radio Frequency Identification) projects in 2009.\textsuperscript{35} In both cases, PIAs were encouraged as best practice, and a means of demonstrating compliance with data protection laws. Since the ICO's handbook, national authorities have published PIA guidelines in several other EU member-states, including Spain, Finland, Germany, and Slovenia.

Most of this activity in Europe had been pursued on the basis that PIAs are recommended but not required.\textsuperscript{36} However, in 2012, the Commission proposed the new GDPR, which would make impact assessments mandatory in certain 'high risk' contexts.\textsuperscript{37} The Parliament stated that impact assessments 'are the essential core of any sustainable data protection framework'.\textsuperscript{38}

Impact assessments may soon go from being a purely voluntary tool to a mandatory requirement in Europe – at least, for certain kinds of data processing – in less than a decade. Why has the Commission taken this approach? Is it likely to succeed, or is this transformation misguided? To answer these questions, it will help to consider what kind of regulatory instrument a mandatory impact assessment might be, and the merits and problems associated with it.

3. Regulatory theory of impact assessments

In the existing literature, impact assessments in the contexts of privacy and data protection

\textsuperscript{35} The idea that the handbook catalyzed PIA use in Europe is suggested in ibid., 2.
\textsuperscript{36} Apart from the aforementioned cases where member states impose mandatory requirements on public bodies to conduct PIAs
\textsuperscript{37} This change has been widely regarded as replacement to the old system of notification, which was regarded as onerous and indiscriminate – see Pederson, A. (2005). Notification - what is the point? Privacy Laws & Business United Kingdom Newsletter, 20(7).
\textsuperscript{38} Recital (71a)
have been mainly been discussed in relation to three broad, traditional categories of regulatory approach: legal regulation, self-regulation and co-regulation.

Unfortunately, there is no generally accepted framework or standardised terminology in the field of regulatory theory which might give these terms a single precise definition.\textsuperscript{39} Regulatory theorists typically conceive of different regulatory approaches as existing on a spectrum between 'pure' legal regulation and 'pure' self-regulation.\textsuperscript{40} Legal regulation is often understood as regulation by the state in the form of legal rules backed by criminal or civil sanctions; an approach sometimes referred to (usually pejoratively) as 'command and control'.\textsuperscript{41} Self-regulation, by contrast, might be characterised as commitments that private actors make for themselves, without any form of enforcement from the state or other external actors.\textsuperscript{42} Between these two extremes lie various terms denoting different configurations of state and private activity, including 'co-regulation', which is generally used to denote various kinds of collaboration between state and private actors in some aspect of the regulatory process, where there is at least some form of legal enforceability.\textsuperscript{43}

PIAs have traditionally been pursued as a self-regulatory instrument. Proponents have often suggested that the benefits of PIAs – such as the mitigation of reputational damage and other risks – ought to be sufficient to motivate many organisations to undertake them of their own

\textsuperscript{39} See e.g. Richards, K. (2000). Framing Environmental Policy Choice. Duke Environmental Law & Policy Forum, 10, 221–85., which catalogues the many different terms used by different authors to refer to the same kind of regulatory instrument.


\textsuperscript{42} Although there are a multitude of different varieties of self-regulation. For a thorough discussion, see ibid., 56.

The perceived merit of this self-regulatory approach is that organisations are free to develop PIA processes which best suit their specific circumstances. It is suggested that this will allow PIA practice to develop flexibly and organically to suit the needs of data controllers. They are therefore described as an example of 'reflexive best practice', in contrast to the 'sledgehammer' approach taken in other areas of data protection policy.\textsuperscript{45}

The main reason for making PIAs mandatory seems straightforward. Unless PIAs are made a mandatory requirement, their use will be confined to those organisations who are already motivated to comply, leaving the risks arising from the processing operations of other organisations to continue unmitigated. If PIAs are indeed as effective at mitigating risks as their proponents claim, regulators ought to ensure they are adopted wherever appropriate. This appears to be the primary argument made by David Wright, in an article in favour of mandatory PIAs published in 2011, prior to the first proposal for the GDPR.\textsuperscript{46}

### 3.1 Mandatory PIAs as legal regulation: would they suffer the drawbacks of 'command and control' regimes?

Making PIAs mandatory clearly changes their status as a self-regulatory instrument. This would appear to place them in the category of traditional legal regulation; a requirement created through state legislation, enforced by regulators through fines, giving little discretion to regulatees. This opens them up to a set of common critiques associated with so-called command-and-control approaches, including the risk that they become “exercises in legitimisation rather than risk assessment.”\textsuperscript{47}

Concerns about bureaucracy have also already

\textsuperscript{44} Ibid., 8., p15

\textsuperscript{45} Brown, I., & Marsden, C. (2013). Regulating code: Good governance and better regulation in the information age (pp. 1–25).


\textsuperscript{47} Ibid., 63.
been expressed by some member states, and industry who suggest that mandatory PIAs may entrench a command-and-control approach, becoming a 'box ticking' exercise, undermining their intended purpose. It is generally recognised that rule-based, coercive and punitive methods applied solely by regulators tend to lead to 'ritualism' (following rules without understanding why they are there), and 'creative compliance' (following the letter of the rules in such a way as to undermine their overall purpose, as in elaborate tax avoidance schemes). The fear is that mandatory PIAs will focus more on demonstrating compliance with specific procedures rather than on flexible, substantive, and holistic risk assessment and mitigation. One only has to look to other contexts in which conducting an impact assessment was made mandatory, as in US and Canadian public sector organisations, to see what has been described as an overly prescriptive, formulaic system, 'devoid of any content of significance to privacy protection, beyond the narrowly circumscribed legal requirements'.

3.4 PIAs as 'co-regulation'

Advocates of mandatory PIAs have a different perspective. They tend not classify the mandatory impact assessment regime as traditional legal regulation. Instead, they see it as as

---

48 The Council noted that 'FR, RO, SK and UK warned against the considerable administrative burdens flowing from the proposed obligation.' (GDPR, Chapter IV, footnote 251).
52 'I fear that, … mandatory data protection impact assessments will function as paper checklists that controllers duly fill in, tick off, and file away to duly show to auditors or supervisory authorities if they ever ask for it. Procedure followed, problem solved' ibid., 67.
53 Ibid., 23.
an effective middle-ground,\textsuperscript{54} that may even ‘obviate the need for “hard” law’.\textsuperscript{55}

This is understandable in so far as the supposed dichotomy between legal regulation and self-regulation is increasingly seen as too simplistic,\textsuperscript{56} with potentially effective measures lying between the two ‘extremes of absolute discretion and total control’.\textsuperscript{57} But in what sense are PIAs 'co-regulatory' if the requirement to conduct them is imposed top-down, and punitively enforced by the regulator? On the other hand, if the measures outlined in PIAs are defined by data controllers themselves, rather than imposed by regulators, then do they really differ from mere self-regulation? The supposed middle ground promised by the term ‘co-regulation’ therefore requires further articulation.

As previously noted, there is unfortunately little clarity over the meaning of terms like 'co-regulation'.\textsuperscript{58} It is a term that obscures a lot of important detail. For instance, it is sometimes used to describe cases where statutory backing is added to pre-existing forms of self-regulation by industry bodies.\textsuperscript{59} In other cases, it denotes attempts by regulators to steer competitive market forces towards the pursuit of regulatory goals, such as with transparency

\textsuperscript{54} For example, Andrew Charlesworth argues that “there has also been a politically-inspired tendency to polarise the data protection debate in terms of a stark choice between command and control regulation or self-regulation” Charlesworth, A. (2006). The future of UK data protection regulation. Information Security Technical Report, 11(1), 46–54. p48.


schemes, audit-backed certificates or mandatory labelling. In yet others, regulators set punitive fines for those who fail to reach certain targets, but allow regulatees significant discretion in devising their own strategies for meeting those targets. A minimal requirement ought to be the involvement of at least some element of legal enforceability, otherwise the arrangement would be indistinguishable from mere industry self-regulation; but exactly what that element should be is often unspecified.

An account is therefore needed of what a ‘co-regulatory’ approach really means in the context of the mandatory impact assessment regime of the GDPR. To this end, we may find clarification by assessing the Commission's motivations and the provisions that appear in the GDPR.

4. Analysis of mandatory impact assessments in the GDPR

4.1 Commission reports prior to the 2012 proposal

The Commission's rationale for incorporating a mandatory requirement for impact assessments can be gleaned from several documents published in the lead-up to the proposal of the GDPR in 2012.

The first is a study commissioned between 2008-2009, which sought to 'identify the challenges for the protection of personal data produced by current social and technical phenomena', such as 'ubiquitous personal data collection' and 'profiling'. According to the study, these new phenomena 'threaten to make the application of the [data protection] principles yet more difficult'. It claims that many organisations do not 'pay appropriate

60 Ibid., 56, p. 4.
62 See (European Commission, 2010b) p. 9
63 Ibid, p. 15
attention to the privacy implications of new information systems before they are commissioned'.

In response to these challenges, the report mentions PIAs as a potential solution, noting the existence of mandatory PIA schemes in other jurisdictions. It notes that for some established data protection measures, including PIAs, 'there have so far been insufficient incentives for their use by data controllers'. Hinting at the regulatory approach that might eventually be adopted through the GDPR, it argues that PIAs would need to be pursued with 'the right combination of law and self- or co-regulatory rules and mechanisms'. In advocating a mixture of different rules and mechanisms to support PIAs, the report indicates sensitivity towards the dangers of adopting traditional legal or self-regulatory approaches.

In a communication published in 2010, the Commission went on to discuss incorporating impact assessments in the new regulation. It describes plans to 'explore ways of ensuring that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules', one of which is the use of what they call 'Data Protection Impact Assessments'. The communication recommends only making them mandatory in 'specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures'.

Potential substantive differences between this new term – ‘Data Protection Impact Assessments’ – and PIAs are significant. While PIAs are more general in nature, encompassing a wide range of data protection measures, the GDPR’s focus is on the specific context of processing personal data. The GDPR requires data controllers to conduct a risk assessment to determine whether the proposed processing activity poses a risk to data subjects. If so, the data controller must implement additional safeguards to mitigate those risks. The GDPR also requires data controllers to report data breaches to the relevant supervisory authority within 72 hours.

---

64 Ibid, p. 50
65 Ibid, p. 51
66 Ibid. p. 46
67 Ibid, p. 56
69 Ibid. p. 12
Assessments’ – and the older term *privacy* impact assessments (PIAs) are not discussed by the Commission. However the changing terminology emphasises the basis of these assessments in *data protection law*. This suggests a redirection of the focus away from privacy *per se*, and towards data protection.\(^70\) Furthermore, the focus on ‘legal compliance’ suggests that the primary aim of a DPIA is to ensure that processing is consistent with the law as defined in the GDPR. This is in contrast with the idea, promulgated by certain proponents of impact assessments, that they should go beyond legal compliance and address general ethical norms about privacy and personal data. In this sense, DPIAs are closer to *legal compliance assessments* than the kind of holistic PIA envisioned by some of their proponents. However, as subsequent sections shall describe, the DPIA requirements are also more substantive than the aforementioned very narrow PIAs required in the US and Canada.

### 4.2 The proposed GDPR

This rationale filtered through into subsequent draft proposals for the GDPR, where the requirement for impact assessments was laid out in detail. The requirement has changed somewhat over the course of revisions between the Commission's original proposal text (published January 2012), the amended version from the Parliament's LIBE committee (confirmed in March 2014), the version published by the Council to outline their 'general approach' (adopted June 2015), and the final version (published July 2016). The initial Commission proposal set out the main provisions relating to impact assessments in Article 33 (Article 35 in the final text), where the overall rationale of 'enhancing the data controller's responsibility' is cited. What follows discusses some of the main elements of the impact assessment proposal, particularly those which are relevant to the question of which regulatory

---

\(^70\) Whether this change in focus should be seen as a narrowing or broadening of scope depends in part on the relationship between data protection and privacy; i.e. whether the former is a subset of the latter, or vice-versa, or indeed whether ‘data protection is both narrower and broader than privacy’ as claimed in (Gellert & Gutwirth, 2012, p. 269-270)
approach they embody.

4.2.1 When are impact assessments required?

Article 35 sets out that impact assessments are only mandatory in certain circumstances, where processing is likely to result in 'high risk to the rights and freedoms of natural persons'. The LIBE committee made some amendments to the Commissions' original proposal, to further determine the situations in which an assessment should be conducted, and the elements to be assessed. In particular, impact assessments would specifically be required for profiling and sensitive personal data.\footnote{LIBE committee amendments 259 and 260 respectively.} These amendments aimed to enhance legal certainty by clearly stipulating 'which specific risks pertain, in an exhaustive manner'.\footnote{Ibid., amendment 258.} Generally, impact assessments would be required in situations of uncertainty, where processing operations 'are of a new kind' (Recital 89). The exact definition of 'high risk' remains to be seen, but a particularly ‘high’ risk threshold could potentially exempt a great deal of processing operations.

To help data controllers ascertain whether a processing operation is likely to present high risks, supervisory authorities will maintain a list of processing operations which are likely or unlikely to present such risks. The 'European Data Protection Board' (a successor to the Article 29 Working Party, established under the GDPR) will ensure these lists are consistent between national supervisory authorities (Article 64 (1a)).

When an impact assessment of a proposed project reveals that high risks exist, data controllers must consult with the supervisory authority (Recital 84). The impact assessment must be included in the communication between controller and supervisory authority. The supervisory authority may then come to the opinion that the intended processing would not be compliant, and use their powers (defined in Article 58 (2f)) to temporarily or indefinitely ban
the processing.

In combination with the test for determining whether an impact assessment is required, controllers therefore face a multi-step procedure based on the processing type. This aims to help both data controllers and regulators efficiently prioritise their attention on projects which require greater scrutiny. This rests partly on the detailed lists to be drawn up by supervisory authorities, but where these do not provide a clear guide, the controller must decide for themselves on the basis of the guidance in Article 35. Further deliberation from the supervisory authority may then occur to determine if the processing will ultimately proceed. The GDPR thus establishes a triage system based on a mixture of regulator and regulatee deliberation.

4.2.2 Scope and content of an impact assessment

The Commission proposal outlines in general terms the aspects that an impact assessment should encompass. These include a 'general description of the envisaged processing operations', an 'assessment of the risks to the rights and freedoms of data subjects', and 'the measures envisaged to address the risks, safeguards, security measures and mechanisms' (Article 35(7)). Initially, the Commission wanted to be able to specify the standards and procedures for carrying out, verifying and auditing impact assessments (Article 33(6-7) in the Commission’s January 2012 proposal text), but this was opposed by both Parliament and the Council in their revised versions.

The Parliament's LIBE committee's amendments attempted to further define the scope and content of an impact assessment. They explicitly included consideration of the 'risk of discrimination being embedded in or reinforced by the operation'; 'existing guidelines'; the use of 'modern technologies and methods that can improve citizens' privacy' (amendment 261); and appropriate means to gain a data subject's consent (amendment 113, (Article 7(1a))).
The LIBE amendments did not end up being included verbatim in the final text, although they are alluded to in the recitals. This leaves open the potential that the content of an impact assessment may be limited by a very narrow interpretation of the notion of risks to ‘the protection of personal data’. However, the requirement that an impact assessment must consider the risks to the rights and freedoms of natural persons (Article 35(7b)) is elaborated upon in Recital 75, which outlines risks such as discrimination, reputational damage and economic or social disadvantage. The fact that such content has been relegated to recitals, rather than included as operative provisions, is regrettable; however, since the GDPR’s recitals are likely to be extensively used by the European Data Protection Board in its application of the consistency mechanism, they may prove to be important as the GDPR unfolds in practice.

4.2.3 Stakeholder consultation

Initially, there was a strong role for data subjects to play in the formulation of impact assessments. The Commission's original proposal would require the impact assessment process to involve a consultation with data subjects (Article 33(4)). The Parliament’s text argued that this ‘represents a disproportionate burden on data controllers’ (amendment 262). In the final text, there is a highly qualified requirement (Article 35(9)); consultation is only required ‘where appropriate’ and ‘without prejudice to the protection of commercial or public interests or the security of the processing operations’.

4.2.4 Fines and ongoing compliance

Article 83 details the administrative sanctions that may be imposed on data controllers by supervisory authorities. There are three tiers of fines. Failure to undertake an impact assessment in violation of article 35 could incur the highest tier of fines, up to €20,000,000 or 4% annual turnover (Article 83(5)).

The Commission's original proposal did not include any provisions to ensure that a controller
adhered to the measures outlined in their impact assessment; but as the LIBE committee noted, 'impact assessments can only be of help if controllers make sure that they comply with the promises originally laid down in them' (amendment 48, recital 74a). To deal with this danger, the Parliament’s first reading position suggested a bi-annual 'compliance review' requirement, to ensure that impact assessments would be an ongoing commitment (amendment 130). The final text states, instead, that such reviews should be conducted merely ‘where necessary’, ‘at least where there is a change of the risk represented by processing operations’ (Article 35(11)). Conducting and monitoring compliance with impact assessments would be a key duty of an organisation's data protection officer ('DPO'), which certain organisations will be required to employ (Article 39(1c)).

**4.3 Summary of the GDPR rationale and provisions**

Mandatory impact assessments differ from traditional prescriptive legal regulation; they are a combination of rules prescribed by the regulator, and policies that the regulatees must devise for themselves and impose upon themselves (with input from stakeholders). The proposal therefore has elements of legal regulation, but with a heavy emphasis on controllers coming up with their own measures.

**5. Meta-regulation as a model of mandatory impact assessments**

As noted above, the term 'co-regulatory' doesn't really distinguish this particular approach from the many other approaches that fall between traditional legal regulation and 'pure' self-regulation. What is needed is an account of how this particular kind of measure – enforced risk-assessment, and compliance with self-imposed, stakeholder-influenced policies – is supposed to work. In what circumstances are such approaches successful? I propose that the GDPR's impact assessment regime can be categorised as an instance of 'meta-regulation', a
5.1 Introducing meta-regulation

Meta-regulation can take many forms. Parker defines it very broadly as 'any form of regulation (whether by tools of state law or other mechanisms) that regulates another form of regulation'. However, the primary interest for Parker (and many others who use the term) is a particular form of meta-regulation, namely the 'legal meta-regulation of internal corporate self-regulation'. In other words, meta-regulation as a means for the state to make corporations responsible for their own efforts to self-regulate. In what follows, I will use the term with this more specific meaning in mind.

For Parker, one main advantage of meta-regulation over other forms of regulation is that it latches onto companies' inherent capacity to manage themselves, but without letting them off the hook if their self-regulation efforts fall short of regulator (and stakeholder) expectations. Meta-regulation differs from self-regulation because its targets don't have the option of not setting up their own rules; individual regulatees are forced to actively self-regulate. Rather than imposing particular rules or technologies on organisations from above, meta-regulation leverages their existing management structures and internal bureaucratic processes in the pursuit of regulatory goals. Companies may be forced to evaluate and report on their own self-regulation strategies so that regulatory agencies can determine whether the ultimate substantive objectives are being met.

---

73 See ibid., 5
74 Ibid., 98.
76 Ibid, p. 8
77 Ibid, p. 13
Meta-regulation must go hand-in-hand with what Parker calls the 'triple loop' of evaluation, which allows regulators and external stakeholders to play an essential evaluative role. The regulator must connect 'the private capacity and practice of corporate self-regulation to public dialogue and justice', by requiring 'companies to gather and disclose information on which corporate self-regulation and its impacts can be judged (by regulators and stakeholders)'. In Parker's view, this introduces a democratic dynamic: 'in a democracy stakeholders need access to corporate reports of their self-evaluation of their own self-regulation, including how they have identified, prevented and corrected problems'.

Parker identifies three approaches to fostering meta-regulation; 'building compliance leadership', 'process regulation', and 'education and advice'. The appropriate approach depends on the stage of development of the particular industry and particular regulatees within it. The most relevant for our purposes is the second - 'process regulation' - whereby government teaches regulatees to self-regulate by forcing them to go through processes that serve regulatory goals. This doesn't mean government prescribing the details of the process or mandating precise outcomes, but it does require organisations to take a systematic approach to identifying, controlling and minimising risks.

Examples include occupational safety or food regulations which require firms to engage in their own processes of hazard identification, risk assessment and risk control. This allows a tailored approach rather than one-size-fits-all regulatory strategy, and gives organisations a chance to integrate regulatory goals into their other business goals and operating procedures.

### 5.2 Impact assessments as meta-regulation

My aim in this section is to demonstrate that the GDPR's mandatory impact assessment

---

79 Ibid., 98, p. 289
80 Ibid, p. 291
81 Ibid., 98, p. 27
regime has many of the hallmarks of meta-regulation, particularly of the kind that Parker outlines. The constitutive features of meta-regulation are manifested in various ways in Article 35 and elsewhere (although, as previously mentioned, I am not claiming that the policymakers who formulated the GDPR were consciously pursuing a meta-regulatory approach as formally described in the academic literature). Table 1 summarizes the constitutive features of meta-regulation, drawn from Parker 2002, alongside the ways that those features are manifested in the GDPR’s impact assessment regime.

**Table 1: Constitutive features of meta-regulation in the GDPR regime**

<table>
<thead>
<tr>
<th>Constitutive feature of meta-regulation</th>
<th>Manifestation in the GDPR regime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires organisations to take responsibility for their self-regulation efforts</td>
<td>DPIAs require data controllers to assess and mitigate risks themselves (Article 35(1))</td>
</tr>
<tr>
<td>Requires organisations to undertake risk-assessment processes</td>
<td>A DPIA should encompass an evaluation of the risks to the rights and freedoms of individuals (Article 35(7c))</td>
</tr>
<tr>
<td>Requires organisations to identify risk mitigation strategies</td>
<td>A DPIA should involve a description of ‘the measures envisaged to address the risk’ (Article 33(7d))</td>
</tr>
<tr>
<td>Does not prescribe specific measures or technologies</td>
<td>No particular measures are prescribed – the controller must identify measures by themselves</td>
</tr>
<tr>
<td>Holds organisations accountable for adhering to their own policies</td>
<td>Controllers expected to review compliance with the measures set out in their own DPIAs (Article 35(11)).</td>
</tr>
<tr>
<td>Attempts to leverage a corporation's existing management procedures</td>
<td>The GDPR attempts to embed DPIAs in management procedures partly through DPO’s (Article 39(1c))</td>
</tr>
<tr>
<td>Ensures stakeholders can</td>
<td>Controller must seek input from data</td>
</tr>
</tbody>
</table>
democratically engage in evaluating organisations' measures and policies subjects or their representatives when conducting a DPIA (Article 35(9))

Liability to sanctions is related to failure to undertake the process, rather than focusing on the outcome Undertaking a DPIA, especially if it is referred to the supervisory authority for prior consultation, is likely to significantly reduce any penalties for subsequent infringement due to the circumstances outlined in (Article 83(2)).

| Table 1. Features supporting classification of DPIAs as meta-regulation |
|---|---|

On the basis of these parallels, I argue that 'meta-regulation' is an apt description of the GDPR's impact assessment regime, in so far as that regime’s intended workings can be surmised from the GDPR texts released by the Parliament, Council and Commission, and the final text. Of course, when the regime is actually put into practice by supervisory authorities, it may end up working somewhat differently, such that the term meta-regulation becomes a less accurate description. But at present, the term is an apt description of the kind of regulatory approach suggested by my close reading of the GDPR.

It is also worth reflecting further at this point on why meta-regulation is a more appropriate label for the regime outlined in the GDPR than a competing term like co-regulation. Co-regulation is a general term for many different regulatory forms, as described above. While it has often been broken down into more specific sub-categories (such as Bartle and Vass’s ‘devolved’, ‘delegated’ and ‘cooperative’ variants introduced earlier), none of these capture with sufficient specificity what is outlined in the GDPR on DPIAs. Meta-regulation, as Parker, Gilad, and others describe it, has a set of particular constitutive features summarized above.
This is consistent with classifying meta-regulation as a \textit{subset} of co-regulatory strategies (although the argument I make here doesn’t require or imply such a classification). So the GDPR’s DPIA regime may be considered a form of co-regulation, whilst also being referred to more specifically as a form of meta-regulation. The advantage of the latter, more specific classification, is that it allows us to evaluate the regime using the resources that have been developed around it. This significant body of theory, analytical frameworks and empirical findings applies to the DPIA regime in a way that more general work on co-regulation would not. The following section provides an overview of this work.

\section{6 Evaluating meta-regulation}

Numerous empirical studies have been undertaken of meta-regulation in a variety of sectors.\footnote{Case studies where meta-regulation has proved successful (or at least, better than alternatives) include: Coglianese, C., & Lazer, D. (2003). Management-based regulation: prescribing private management to achieve public goals. Law & Society Review, 37.; Ibid., 86; Parker, C., Gordon, T., & Mark, S. (2010). Regulating Law Firm Ethics Management: An Empirical Assessment of an Innovation in Regulation of the Legal Profession in New South Wales. Journal of Law and Society, (37), 466–500.; Ibid., 98. Mixed results were found in: Hutter, M. (2001). Regulation and Risk: Occupational Health and Safety on the Railways. Oxford University Press; Gunningham, N., & Sinclair, D. (2009). On the Limits of Management Based Regulation. Law and Society Review, 2(43), 865–900.} Sectors in which meta-regulation initiatives have been studied include anti-pollution; safety of food, toxics and hazardous chemicals; occupational risk prevention; professional ethics; aerospace and financial services.\footnote{Ibid.} Generally, while results can be varied, meta-regulation appears to make an overall positive contribution to regulatory goals.\footnote{Ibid., p. 104.}

Sharon Gilad has conducted a meta-study of these various empirical case studies.\footnote{Ibid.} On the basis of this meta-study, Gilad introduces an evaluative framework to identify the conditions under which meta-regulation has most chance of success, and where it is likely to fail. Gilad's
framework builds on Parker's version of meta-regulation. The framework proposes that there are several key factors in the success or failure of meta-regulation. I outline these key elements of Gilad's framework below, before considering each of them in relation to the DPIA regime proposed in the GDPR in the following section.

**Leveraging regulates:** Gilad's framework states that meta-regulation is most effective when it leverages regulatees' ability to learn and discover effective measures to achieve regulatory goals. Rather than expecting this to be done by the regulator, who is ill-positioned to uncover the optimal solution for the regulatee's idiosyncratic context, meta-regulation shifts 'the primary responsibility for identifying risks, setting standards, and monitoring compliance to regulated organizations'[^86]. However, there is a danger that the regulatee's apparently superior knowledge results in ineffective solutions. This brings us to the next factor in Gilad's framework: the need for independent scrutiny.

**Independent scrutiny:** Gilad notes empirical studies that suggest meta-regulation is less effective when the regulator is unable to evaluate the efficacy of organisations' risk-management plans. This can be due to uncertainty about how to conceptualise risk, and a lack of knowledge about which mitigation strategies are appropriate[^87]. This could lead to organisations – intentionally or due to ignorance – pursuing strategies that would result in failure, and the regulators would not be in a position to identify their flaws. Meta-regulation therefore 'depends on regulators’ capacity to independently assess and challenge the validity of the information that regulatees generate about their performance'[^88].

Gilad also notes that in addition to well-informed regulator scrutiny, effective meta-

[^86]: Ibid., p. 497
[^87]: Ibid., p. 496.
regulation requires scrutiny from stakeholders.\textsuperscript{89} This helps ensure their values and expertise feed into the regulatory process. These processes need legislative backing; as Parker notes, attempts to make regulatee's activity open to challenge and revision by stakeholders are likely to 'fail badly unless they ... identify and give rights to stakeholders to participate in or contest corporate decisions'.\textsuperscript{90}

**Stability, trust and external support:** A third factor identified by Gilad is the need for 'regulators and regulatees [to] enjoy mutual trust and external political and public support, which would provide them with latitude for short-term experimentation in pursuit of long-term improvements'.\textsuperscript{91} Regulatees need to feel confident that regulators taking a meta-regulation approach will not just 'shift to them the blame for future failure'.\textsuperscript{92}

**Regulatory tiers:** Gilad introduces the concept of 'regulatory tiers' to explain another important factor in the success of meta-regulation.\textsuperscript{93} First-tier operations involve 'detailed rules' and 'outcome-oriented standards', i.e. the traditional focus of prescriptive legal regulation. Second-tier operations concern 'the governance structures and controls that regulatees should have in place in order to audit their compliance with first-tier regulatory requirements'. Third-tier operations focus on the 'evaluation, design, and readjustment of ... first-tier production and second-tier controls'. Based on a meta-analysis of case studies, Gilad concludes that meta-regulation works best as part of a hybrid system. Meta-regulation should be aimed at third or second-tier operations, working in combination with more 'prescriptive and outcome-oriented regulation' aimed at the first tier.\textsuperscript{94}

\textsuperscript{89} Ibid. p 500  
\textsuperscript{90} Ibid., 98, p. 48  
\textsuperscript{91} Ibid., 104, p. 503  
\textsuperscript{93} Ibid., p. 489  
\textsuperscript{94} Ibid., p. 497
Shaping organisation’s compliance: A final factor in Gilad’s framework is the extent to which meta-regulation succeeds in transforming organisations’ compliance and capacity to self-regulate. While prescriptive regulation may be suited to ‘managing non-compliance by a few bad apples’, it is unsuitable ‘where non-compliance is persistent and widespread’. In the latter case, what are required are ‘profound transformation of industries’ resistance to regulation and the constitution of self-regulatory capacity within organizations’. To successfully facilitate such transformation, meta-regulation needs to be capable of shaping organisations’ self-interest and normative commitment.

7. The prospects for DPIAs as meta-regulation

Having explored how the concept of meta-regulation provides an apt description of the DPIA regime outlined in the GDPR, and reviewed the theoretical and empirical literature on meta-regulation, we are now in a position to assess the regime’s prospects in light of this. Is meta-regulation a promising choice of regulatory style in the contexts in which DPIAs are required under the GDPR?

7.1 Leveraging regulatees

The GDPR’s DPIA regime does appear to be designed to leverage regulatees capacity. It attempts to allow room for data controllers to apply their own expertise to a problem. Rather than prescribing the exact measures and safeguards that must be implemented, it requires controllers to identify their own solutions to mitigate risks that are appropriate to their context (Article 35(7d)).

While member state supervisory authorities may reasonably claim superior understanding of the data protection principles, they may not have a superior understanding of the latest personal data processing techniques, nor the most appropriate privacy-enhancing

95 Ibid., p. 498
technologies. For instance, in the case of organisations operating at the cutting edge of data science (an area which may well involve the potentially 'high risk' processing operations covered by Article 35), regulatees are likely to consistently have greater expertise than the regulator.

7.2 Independent scrutiny

The success of a meta-regulatory approach to PIAs will significantly depend on the capacity of supervisory authorities to independently scrutinise data controller's proposed mitigation strategies. The proposed GDPR does attempt to ensure such scrutiny happens. When a PIA identifies 'high risk' processing operations, controllers would have to submit their PIA report to the supervisory authority so that their mitigation strategies can be scrutinised (Article 36(1)). They would also have to submit compliance reviews so that their ongoing compliance can be assessed (Article 35(11)). But an obligation on data controllers to allow their programs to be scrutinised does not guarantee that supervisory authorities will do so competently.

This suggests an important role for the European Data Protection Board, in developing expertise on potential risk identification and mitigation strategies. This could be communicated to supervisory authorities to aid in their consultation processes.

Stakeholder scrutiny is a key part of successful meta-regulation. This is manifested in the GDPR in the requirement to seek input from data subjects or their representatives when conducting a PIA (Article 35(11)). It remains to be seen how effective this measure might be, especially given that is only to be required ‘where appropriate’ and ‘without prejudice to the protection of commercial or public interests or the security of processing operations’; exactly how these terms are interpreted by data protection officers and supervisory authorities will be key. While stakeholders need to be consulted, there is no mechanism within the GDPR which ensures that their views are actually incorporated in the eventual implementation of the controller’s processing operations.
It may also strongly depend on the processes by which data subjects or their representatives are identified and consulted; whether they are truly open or simply a tick-box exercise. And if conflicts arise, it's not clear how they'd be easily resolved; stakeholder engagement may be more likely to produce 'dissent, deadlocks, and stultification rather than action'.\textsuperscript{96} However, Gilad's overview of empirical studies of meta-regulation suggest the opposite. Stakeholder-regulatee deliberation may actually work \textit{better} where such conflict is greater and therefore stakeholder's motivation to participate is higher.\textsuperscript{97} Ideally, regulators need to support stakeholders in holding regulatees to account.\textsuperscript{98}

Such a process is unlikely to lack willing participants in the context of data protection. There is a large, diverse, knowledgeable and vocal privacy advocacy community willing to engage on behalf of data subjects.\textsuperscript{99} In recent years, such groups have expended great efforts in lobbying European regulators over the form of the GDPR and in encouraging their national supervisory authorities to take action against certain companies. In the years that follow, their effort could be re-directed, through a stakeholder-oriented PIA system, into improving the specific activities of data controllers. But realizing this positive potential is dependent on a strong interpretation and enforcement of the Article 35(9) provision, which seems less likely given the qualifications outlined above in the final text of the GDPR.

\textbf{7.3 Stability, trust and external support}

It is uncertain how much stability, trust and external support exists in the context of data protection and PIAs. In terms of its political and regulatory agenda, the EU may provide a

\textsuperscript{96} Ibid., 104, p. 178
\textsuperscript{99} Bennett, Colin J. The privacy advocates. MIT Press, 2010
relatively stable environment. The substantial time and effort involved in creating and implementing the new data protection regulation means that it is likely to stay in place, unchanged, for a long time.

However, the level of trust between regulators, regulatees, and stakeholders, and the general level of external political and public support, may be less than ideal. For instance, recent relationships between regulators and large technology companies (often based outside the EU), have been adversarial and frayed. Attempting to develop a co-operative process may prove difficult given this recent history, but equally, it could offer a much-needed fresh start.

Another important element of trust identified by Gilad is that meta-regulation should not simply shift the blame for future failure onto the regulatee. While they do aim to ‘increase controller’s responsibility’, PIAs are not designed in such a way. If a data controller effectively undertakes an PIA as required, and has faithfully implemented the measures outlined in it, this will be taken into account as a mitigating factor if they later face the prospect of an administrative sanction (Article 79(2b(e))). This ought to create conditions in which responsibility is more fairly apportioned and trusting relationships between regulators and data controllers can be built.

### 7.4 Regulatory tiers

Gilad’s concept of regulatory tiers is an apt description of the relationship between PIAs and other provisions of the GDPR. Many of the GDPR’s provisions, such as the core principles, concern specific rules and outcomes – i.e. ‘first tier’ operations. The provisions on PIAs, by contrast, aim to ensure controllers implement processes for the governance, monitoring,

---

100 See, for instance, recent disagreements between European supervisory authorities and Facebook (Schrems, M. (2014). Kämpf um deine Daten. Verlag.).

101 See GDPR Chapter 2, Articles 5-10
evaluation, design, and readjustment of those first-tier operations. In this respect, PIAs can be seen as second and/or third-tier operations, constituting a complementary layer that sits above the established first-tier data protection rules which are epitomised by a more traditional prescriptive approach. The case studies of meta-regulation assessed by Gilad suggest that this is a common and effective arrangement.

7.5 Shaping organisations' compliance

As with the introduction of mandatory risk assessments in other industries, by requiring data controllers to identify risks and potential mitigation measures mandatory PIAs may help convince organisations of the long-term net gains to be had from investing in compliance.

Gilad also talks of the benefits of certain regulatees acting as industry leaders. There is some evidence that some data controllers do indeed value their status as leaders in the industry and are keen to share their knowledge and risk mitigation strategies. This can be seen in efforts by major industry players to publicise and disseminate their best practices, and initiatives within the privacy profession to elevate the status of industry 'thought leaders'. This bodes well for a meta-regulatory approach which emphasises learning and knowledge transfer between regulatees.

Regarding organizational norms, the introduction of data protection officers (DPOs), trained externally by professional bodies with a strong understanding of and normative commitment to privacy, could have an important effect here on the organisation's norms. The GDPR foresees a clear role for DPO's in implementing successful DPIAs (Article 37.1(f)).

---

102 Of course, in attempting to ensure organisations conduct DPIAs, the provisions do impose specific rules and processes on controllers – but this is done with the aim of instilling third and second tier operations.

103 Ibid., 82, 86.
8 Conclusion

In their early incarnations, PIAs appeared to be part of a self-regulatory approach to data protection. In making DPIAs a mandatory requirement under the GDPR, European regulators took them in a different direction. It is understandable that some might fear this change of direction would result in the regulatory pendulum swinging too far the other way; an entrenchment of the command-and-control approach and a re-encroachment of the state.

However, advocates of mandatory PIAs have suggested they can be a cornerstone of a new 'co-regulatory' approach. As we have seen, this term provides little clarity and fails to explain how mandatory PIAs can avoid the typical problems associated with either traditional command-and-control regimes or self-regulation. I have therefore suggested that meta-regulation provides a more accurate description with which they can be better understood and an evaluative framework within which they can be assessed.

Meta-regulation is offered here both as a descriptive account of the mandatory PIA regime laid out in the GDPR, and also as a normative ideal to which policy-makers can aspire.

Seeing mandatory PIA regimes as a form of meta-regulation allows us to make sense of the Commission's proposals, as well as outlining their potential benefits and suggesting the kinds of challenges that they might face. Meta-regulation aims to make organisations responsible and accountable for their efforts to self-regulate, and create a triple-loop evaluative process in which stakeholders can exert influence. By following this approach, mandatory PIAs could allow both the flexibility associated with self-regulation, and the benefits of external pressure associated with legal regulation.

Applying Gilad's framework for assessing meta-regulation to the GDPR's proposed provisions on DPIAs brings to the fore some potential benefits and likely challenges. The GDPR's DPIA regime is strong on several aspects of Gilad's framework, including: the prospects for leveraging the effort and expertise of regulatees; the stability of the regulatory
regime; the appropriate use of regulatory 'tiers' in a hybrid model; the capacity to engender better compliance norms and introduce new compliance incentives. In each of these respects, the DPIA regime proposed in the GDPR appears to accord with successful implementations of meta-regulation in other sectors.

However, the regime is likely to face challenges in other respects. Many of the provisions and amendments proposed in earlier drafts, which would have had a strong chance of embodying the meta-regulation ideal, have been watered down in the final version of the text. The capacity for sufficient independent scrutiny by supervisory authorities is uncertain. Trust between regulators and regulatees, and the level of political and public support, may be shaky. Transforming compliance cultures within organisations is a fundamentally complex and unpredictable process. Finally, while stakeholders have certain rights to participate in the DPIA process, these are highly qualified and the GDPR does not guarantee that controllers will facilitate meaningful input from them.

Any hopes for a functioning meta-regulatory impact assessment regime now depend on the guidance that supervisory authorities develop on compliance with Article 35. How they elaborate upon the ambiguous qualifications contained within the article will prove crucial. Efforts should be made to ensure that the requirement to engage stakeholders is upheld. Commercial, public and security interests should not be used as an excuse to avoid engagement. Successful engagement exercises may not always need to involve disclosure of the specific design of proprietary algorithms; often a broad outline of the technology and its effects will suffice. The reports generated during an impact assessment should also be made available to data subjects wherever possible (even if redactions are necessary in some cases). Supervisory authorities should also take a strong stand on the need for ongoing compliance with and periodic reviews of impact assessments. What exactly constitutes a ‘change in the risks’ involved in processing (as referred to in Article 35 (11)) should be fleshed out with a (non-exhaustive) lists of examples. In monitoring changes to the risks of their processing
operations, controllers should be expected to consider not only changes resulting from their own internal policies and projects, but also new risks arising as a result of external technological developments, new security vulnerabilities and social changes.

With this approach, impact assessments have the potential to be not just another hoop for data controllers to jump through, nor yet another way for organisations to cover their backs and avoid liability. In theory, they can add an additional layer which brings responsibility for considering and deliberating on risky and complex data protection issues into the open. They attempt to make the grey areas, which organisations have so far been left to deal with behind closed doors, permeable to external assessment and influence. The success of a meta-regulatory approach is by no means guaranteed, but it is an ideal that regulators would do well to strive towards.