Regulatory compliance and over-compliant information sharing – Changes in the B2G landscape

Klievink, Bram; Janssen, Marijn; van der Voort, Haiko; van Engelenburg, Sélinde

DOI
10.1007/978-3-319-98690-6_21

Publication date
2018

Document Version
Final published version

Published in
Electronic Government - 17th IFIP WG 8.5 International Conference, EGOV 2018, Proceedings

Citation (APA)
Klievink, B., Janssen, M., van der Voort, H., & van Engelenburg, S. (2018). Regulatory compliance and over-compliant information sharing – Changes in the B2G landscape. In *Electronic Government - 17th IFIP WG 8.5 International Conference, EGOV 2018, Proceedings* (pp. 249-260). (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 11020 LNCS). Springer. https://doi.org/10.1007/978-3-319-98690-6_21

Regulatory Compliance and Over-Compliant Information Sharing – Changes in the B2G Landscape

Bram Klievink(✉), Marijn Janssen, Haiko van der Voort, and Sélinde van Engelenburg

Delft University of Technology, Delft, The Netherlands
{A. J. Klievink, M. F. W. H. A. Janssen, H. G. vanderVoort, S. H. vanEngelenburg}@tudelft.nl

Abstract. Business-to-government information exchange has over the past decades greatly benefited from data exchange standards and inter-organisational systems. The data era enables a new shift in the type of information sharing; from formal reporting to opening up full (and big) data sets. This enables new analytics and insights by government, more effective and efficient compliance assessment, and other uses. The emphasis here shifts from establishing formats to deciding what information can be shared, under what conditions, and how to create added value. There are numerous initiatives that explore how to put data to better use for businesses, for government and for their interactions. However, there is limited attention to exactly how these new forms of extensive data sharing affects the supervision relationships. In this paper, we exploratively look across three research projects to identify the implications of information sharing beyond the regulatory requirements ('over-compliant'). We find that the lack of attention to those implications lead to solutions that are hard to scale up and present unexpected consequences down the line, which may negatively impact the future willingness to explore new potential added value of data sharing.

Keywords: Business-to-government · B2G · Regulatory compliance Supervision · Information sharing

1 Introduction

Ever since their inception, information and communication technologies (ICTs) have played a big role in inter-organisational information exchange. We are here concerned with a specific domain for information exchange; that between businesses and government (or B2G information exchange). Electronic B2G information exchange is useful for all kinds of data that businesses must provide to government, for example for supervision purposes, taxation and statistics. Companies must comply with many laws and regulations and the information they collect and hold can be vital in demonstrating compliance to government actors and other stakeholders [1, 2]. ICTs help companies collect evidence about compliance and support the exchange and evaluation of that evidence. The added efficiency that this brings, has been one of the main drivers for interoperability, standards and inter-organisational systems in this domain. To

P. Parycek et al. (Eds.): EGOV 2018, LNCS 11020, pp. 249–260, 2018.
https://doi.org/10.1007/978-3-319-98690-6_21

demonstrate compliance, the way that companies themselves collect and process information requires certain controls and standardised formats and access by government [3, 4]. Such B2G reporting is highly regulated, with obligations pertaining to scope, scale, timing and format for sharing. Standardised data formats and interfaces as well as regulatory and supervisory instruments such as EDP auditing, play an important role in how ICTs assist companies in demonstrating compliance - and governments in assessing it. The introduction of electronic data exchange several decades ago, can be seen as the tipping point for digital B2G exchange. Many e-government systems that are meant to collect or receive business information accept documents according to standardised data and messaging formats. These highly structured, yet age-old formats are still widely used due to their large installed base. Yet, we can now witness a new tipping point based on the increasing amount of data and the technical capability to share and act on original source data in near real time.

There is a host of enterprise information systems (EIS), monitoring systems and inter-organisational systems (IOS) that all collect, produce and/or store information. This information is not just key to the operations of the company, governments can also use the information. Scholars, companies and government are now working on new ways of information sharing, that are based on applying the same formats and systems for both business operations and B2G, instead of B2G exchange being a derivative of the full source data as they exist in the enterprise systems [1, 2]. This allows piggy-backing on original business data by governments [5] and that support new value creation by going beyond the formal reporting and compliance relationship [6]. The emphasis then shifts from the old practice of identifying formal data elements and reports, to identifying and deciding which information may or should be shared to create value for regulatory supervision and/or other purposes. It may even enable governments to do data analytics and identify patterns that they otherwise could not. We summarise this as "over-compliant" information sharing, by which we mean that businesses open up more information than that they are legally required to.

Although over-compliant B2G information sharing is technically feasible and looks promising, a significant part of the 'business case' is related to innovation in supervision that are enabled by it. A prominent example here are companies that share original business records with more information than is formally required, who may be 'rewarded' with less inspections or a lower administrative burden. However, the work on such innovations do mention but rarely focus on the implications of additional data sharing on the compliance and supervision relationship between the parties involved. The work that does address this topic, often does that from the perspective of a single case or project in which over-compliance (our term) plays a role. This paper aims to address this gap by exploring three projects on over-compliant B2G information sharing and what that means for the relationship for the relationship between the companies and supervision or oversight bodies. To this end, we study three research projects on over-compliant information sharing and look for insights across those cases to identify the implications that such forms of sharing may have on B2G information exchange. Specifically, we do that from a perspective of regulatory compliance based on B2G information sharing.

The paper is structured as follows: in the next section, we discuss the current paradigm of B2G information sharing, which heavily relies on inter-organisational

systems and standardised information exchange. We also there discuss the recent literature on over-compliant information sharing. In the third section, we briefly explain our approach and the three projects we study. In Sect. 4, we present our findings. Finally, in Sect. 5, we summarise those in terms of conclusions.

2 Background

There are many considerations for businesses to (not) share data with government. For instance, technical considerations and capacity considerations, the risks of data ending up with competitors, and the risk of sharing inaccurate data seem to be relevant. From a more political viewpoint, being transparent towards a regulator might put the business in a vulnerable position for the obvious reason that regulators may have enforcement instruments that may hurt the business. This way of opening up may involve risks to the business and the way businesses want to manage these risks are relevant for regulators seeking compliance. As we are interested in the relationship between over-compliant B2G information sharing and regulatory governance, in this section we discuss the relevant background of both. We first dive into how IT supports and changes this relationship. The main part of this section follows after that: we discuss regulatory governance literature to find the main context variables that affect compliance and the relationship between supervision agencies and businesses.

2.1 Information Sharing

The introduction of information systems has greatly transformed the practice of information exchange between businesses and governments. Governments have put in place information systems for exchanging data with companies, including data for taxation, business reporting, statistical purposes, and for establishing compliance to relevant policies and regulation. Many of these systems are directly relevant for operational processes at both the business and the government side. Hence, their operations become mission-critical to at least some of the organisations involved. Pressing impediments and project risks are salient and need to be addressed [7–9]. The antecedents of use of information systems has been a topic of interest for a few decades now [10]. Among the key factors that influence adoption and diffusion of IOS, are the characteristics of the system, their benefits, institutional forces, resource dependence and readiness [10]. The implications on the organisation are often profound and may require restructuring of the organisation and changes in and standardisation of the information function in the organisation to adapt to inter-organisational information sharing landscape. As ICT may reinforce dependencies, organisations may be hesitant to deeply integrate them in their own systems, for example to avoid a lock-in by partners [11]. Trust in sharing partners is key to reap full benefits yet is difficult to develop. Even though this may be less of a problem in B2G information sharing, at least some of the information shared with governments will depend on information of (trading) partners and also the risks and benefits may be at the network level instead of at the level of the individual organisation [12]. In sum, B2G information sharing used

to be mainly about standardised information exchange via interoperable systems, to enhance efficiency in reporting and processing data.

In the current day and age, the information flow from business to government can be based directly in business information systems or allowing governments to tap into information flows that are used for multiple purposes [1, 5]. To enable this shift, internal and external control over companies' operations are crucial. As many operations are at least supported by information systems, the control objectives also concern the information systems [3]. Forms of over-compliant B2G information sharing, as presented in the introduction [5, 6] present challenges that may alter the relationship between regulator or supervision agency and the company providing the information. Studies that touch upon over-compliant information sharing often acknowledge that this is the case, yet rarely cover this change thoroughly. The benefits are often phrased as: re-using data collected for other purposes saves costs, sharing more information allows supervision bodies to make better decisions which would lead them to not burden over-compliant companies, and there might also be reputational gains [3, 13, 14]. At the same time, new incentive schemes are surely required, as companies typically incur costs and are susceptible for additional risks if they give more detail than necessary. But then what does over-compliant information sharing mean for compliance and the supervision by governments?

2.2 Compliance and Supervision

This subsection covers the literature on regulatory compliance and takes a political view. In the literature, we distinguish five context variables: (1) Compliance motives of the regulated, (2) Compliance enforcement strategies of the regulator, (3) Compliance relationships, (4) Public compliance regimes, (5) The broader institutional context.

Compliance motives of the regulator is a classic concern in regulatory literature. Kagan and Scholz made an authoritative typology of regulated businesses informed by both their motives and capabilities to comply [15]. The typology includes "amoral calculators" and "political citizens" as businesses that under some conditions are non-compliant. The first is informed by their own interest and the second with the moral ambivalence or regulation [16]. A third type of non-compliant business as identified by Kagan and Scholz are the "organisational incompetent", being those that might want to comply, but are not able to. The willingness and ability to comply may not only determine the eagerness to open up. The motives also suggest that the decisions what to share and how to share it are in their core of a strategic kind. If these decisions are perceived this way, data and sharing methods become strategic assets.

Compliance enforcement strategies. From the side of the regulator the enforcement style is relevant to the tendency of businesses to share data. In regulatory governance literature two main styles are distinguished [16–18]. A first is the classic style of enforcing the law if a business violates it. This style is usually coined as deterrence [15, 19], penalism [20], coercion or the sanctioning style [21]. After incidents a call for stricter enforcement is commonly heard, however this strict style is plagued by principal- agent problems since regulators have to rely on data to detect law violations [18, 21]. An alternative style is a coaching style that is more focused on learning by the business, better relations between regulator and business and development of

professional norms to cope with moral ambivalence of rules [18]. These regulatory styles influence the strategic considerations for businesses to share data. The main consideration here is the probable impact of data about law violations on the business. If data show law violations and these violations will automatically result in public interventions such as fines, the regulated wouldn't be too eager to open up.

As a function of both the motive of the business and the style of the regulator, their compliance relationship is a context factor of considerable importance. De Bruijn et al. [21] found a seemingly endless amount of strategies both the regulator and the business have to confuse the other. Since the nineties, regulatory governance literature started to focus on the questions how the relationships between regulator and business can be made more productive – at least for the regulator. Typical topics are the responsiveness of regulators to the behaviour and motives of the businesses [22], the way regulators interact with their regulatory counterparts within business such as compliance managers (Parker) and the way trust between regulators and businesses evolves [23, 24]. The relevance of these more relational issues is their capacity to make the behaviours around data exchange some more predictable. Some more stability of expectance about what is being done with the data may encourage opening up in the course of time.

A fourth variable is about regulatory policies rather than regulatory styles. On this level, public compliance regimes define the inspector's job. What are the rules the businesses have to comply with? May distinguishes prescriptive regulation, performance-based regulation and system-based regulation [25]. They mainly refer to what the rules prescribe, which are actions, results and processes. These regimes matter for data exchange for at least two reasons. First, per regime, different types of data are needed and some data are more sensitive than others. Second, they imply different responsibilities of the business. For instance, performance-based regimes leave leeway to how results or outcomes are reached [26]. System-based regimes usually refer to management systems the businesses control themselves, and this way aim to reinforce the self-regulatory capacity of the regulated business. As such, these regimes – more than others - imply an own responsibility for businesses to collect compliance data and also imply a role for regulators to drive away from this data collection process and collect data on a metalevel (i.e. is there a management system in place?).

Finally, the broader institutional context of the relation between regulator and industry matter for decisions to share data. The relation between regulator and business doesn't develop in isolation. Regulated industries face many different public and private actors demanding responses, including banks, NGO's, insurance companies, trade organisations, and governments [21, 27]. In the 2000s a 'decentred view' on regulation became in vogue. With such a view government is no longer perceived to act as the central regulator of the public sphere. Regulation is essentially not state-centred, but rather a result of various public and private regulators seeking to impose rules to others [28–30]. From this viewpoint, Black and Baldwin introduced the idea of 'really responsive regulation' [31]. Regulators would not only respond to compliance of regulated firms, but also to their institutional environments, interactions of regulatory controls and change – among other aspects [31, 32]. Data exchange cannot be isolated from its context. If perceived so nonetheless, special effects may happen. For example, media might be eager to publish about business performances based on data offered to governments, sometimes devoid from any nuance [33].

3 Approach and Project Descriptions

This paper is concerned with the implications of over-compliant B2G information sharing on compliance and supervision. Recent work that does address this topic, often does that from the perspective of a single case or project in which over-compliance (our term) plays a role. In this paper, we seek to go beyond that and look across three of such projects to extract a more comprehensive view on the issues that over-compliant B2G information sharing presents for the compliance relationship between government and companies.

The three projects that we focus on are research or research & development projects. That makes sense, as implementing these solutions in practice lead to numerous challenges and issues. The three projects are: SBR (a public-private initiative in the Netherlands), CASSANDRA (an FP7 project), and JUST (a Dutch research project). The first two were active in the beginning of this decade, the latter is an ongoing project. All of them concern the Dutch situation, with the exception of Cassandra, which operated in various European countries (the Netherlands included). Given the explorative nature of this study, we did not employ a rigorous comparative design, yet revisit the documents and papers on these projects to extract what can be learned from them about the supervision relationship. The authors were involved in these projects [1, 2, 6, 12, 34, 35], which hurts replicability but we do trade that off with much in-depth, first-hand information. The study is thus based on participatory observation by the authors in these three projects as well as on the documentation in formal project deliverables and papers published on the projects.

3.1 Description of the Projects

SBR: Standard Business Reporting. The first initiative we reflect on is a Dutch initiative called Standard Business Reporting (SBR). It was developed and applied in the Netherlands to change B2G reporting [1, 2]. The specific issue addressed by SBR is that often companies have to provide similar (although not always the same) information to multiple government agencies, each with their own systems, formats and definitions. This leads to multiple interfaces, and checks on data elements, standards and definitions. Consequently, information is sometimes shared through separate reports (IOS, e-mail), making the extraction of key information a time-consuming and error-prone process. The SBR project delivered a platform that builds on the eXtensible Business Reporting Language (XBRL). A key contribution of the project was to agree on standardization of data (syntax and semantics) [2, 6].

CASSANDRA. Similar to SBR, the many actors that are involved in international trade also report much information to various government agencies as well as to other parties in the chain. As international trade is typically organised in supply chains involving many companies, there are many handovers between those actors, even before the information is supplied to the government by one of them. The information is therefore often fragmented and information quality can be poor [34, 36]. This project focused on leveraging IT innovations to improve the information exchange between actors worldwide by creating electronic connections between organisations. In the project, the systems of supply chain partners are interconnected and jointly formed an

international information infrastructure [5, 34, 37]. Through the infrastructure, data can be shared among supply chain partners as well as with government. Government agencies involved in the supervision of international trade (e.g. customs, food and product safety, tax) can get a better view on the goods actually being traded and entering the country if they can get detailed information from the original source information systems at all of the parties involved in the shipment [6].

JUST. The JUST (JUridical and context-aware Sharing of informaTion for ensuring compliance) project is related to the infrastructures of the aforementioned projects yet focuses on an important development: context-awareness. The other projects did cover important issues on governance, collaboration and trust. However, they typically assume it is a onetime decision for companies; they either stick to formally reporting the information they are required to share, or they decide to open up more data than they are legally required to do. However, the developments towards context-aware systems mean that information gets shared. What that means, may depend on the context. That gives rise to a specific challenge with potentially great implications for B2G information sharing: context information about the requester of access to data, together with relevant business rules, can play a key role in the decision about whether to share data [35]. Also the legality of the sharing of information can depend on various context variables, including the circumstances, jurisdiction, applicable regulations, original source of the data, business relationship between the company and the source, public interest considerations, and many other factors.

Businesses have to take these and other matters into account when deciding to share data with governments beyond their formal obligation. That means that sharing is not a decision that is made for all data and all time, but there are many factors that play a role and those factors may play out differently in different instances. For example, the information that a company shares from the operations in one supply chain may be in much greater detail, than what the same companies shares on operations in another supply chain (with other partners and data from different sources).

4 Findings: Compliance Challenges and Consequences for Supervision

The three projects each paint different pictures of the effects of over-compliant B2G information sharing on supervision. In brief, in SBR big challenges can be found in the interaction among government agencies, in Cassandra we find risks of getting punished for ‘good behaviour’ and in JUST we find that the technical developments towards context-awareness may have some implications. In this section, we discuss these findings, albeit a bit briefly.

Intra-governmental issues. The concept is often presented as an innovation in public-private interactions. In the SBR case, the core components were quickly considered public infrastructure and hence the responsibility of government. That would provide continuity and stability that is needed to make the change systemic to the way businesses store and report information. Furthermore, for some of the services based on the innovation, the law just states that they are the government’s responsibility. Yet,

several market representatives were involved in standard selection, taxonomy creation and decision-making. Apart from this being a challenge on the public-private interface, also within government there are many agencies and other organisations that act as supervisor on a specific area. Many companies have dealings with multiple of them (e.g. tax, customs, food and product safety, financial regulators, etc.) and the file-once principles requires that they are all able to act on the same data, using the same standards, following the same procedures. The lead agency in the project (the tax administration) thus had to make many decisions that would work for them, but also for the companies and other agencies. An important challenge here is what if others decide not to follow, for example because their task is less information intensive? The differences between government agencies is not trivial; legislation does not allow to re-use data collected for one purpose to be used for different purposes. Furthermore, as various agencies have different legal bases (e.g. tax or commercial) for their data requests, reports may use the same data but end up with different interpretations. These issues were also found in the Cassandra case.

Interoperability and openness of data is obviously a key issue when it comes to the information system aspects of the innovation. Yet, there are also major implications for compliance. In the cases we find situations in which data originally comes from third parties (i.e. the reporting company receives this data from a third party as part of their operations). In our cases that concern international trade data, data often gets updated in the business systems, for example as quantities or destinations change. In over-compliant information sharing, supervisors have access to the company data. However, in regulations, there are formal reporting moments (for example entry summary declarations for incoming goods); if data get updated after that formal reporting moment, what is then the status of that information? The update itself is information for the supervisor (both the update and the fact that is was updated), but does the regulatory regime allow the agency to act on that? And what does that mean for decisions based on the earlier data?

There are ***different speeds***, which is especially visible in the SBR case. The first phases were relatively experimental and first movers faced high transaction costs. There were many incentives for businesses to wait and see, as old alternatives may be not efficient on paper, yet were in practice. It is attractive for them to free ride on the investments of first movers. It was to government to show the efficiency of SBR and make it attractive to step in as quick as possible. A catch 22 situation proved to be a risk: the project needed a critical mass of business to participate to mature, while businesses waited SBR to mature. Also among regulators some there were front runners and others were laggards. As a result, front runners are exposed to risk of failure. At the same time, the standards and customs developed by front runners may become de facto standards. The Dutch Tax Administration, as the main proponent of SBR, didn't always wait for other government agencies to participate. For instance, they developed their own system-to-system channel (BAPI), which reduced possibilities to find a collectively rational solution.

The disadvantages. Companies tend to focus on the benefits they might get when sharing additional data. Also for the government agencies, providing supervision-related benefits is key to incentivise companies to open up their information systems. In

practice, however, we found that it is not uncommon that the data that is shared beyond their duty to share, at times also makes errors visible, such as underreporting or misreporting. These errors might not have been detectable under the 'normal' supervision regime, but now lead to fines precisely because of the over-compliance of the company. In the instances where we found this, the companies did not want to be punished for something that is a result of their attempt to be better than others. Also the supervision agencies would rather reward the companies than punish them. Yet, if an inspector finds something wrong, they have no choice but to act on that information, even if provided voluntarily. This shows that the compliance motives of the company are supported by the relationship with the supervisor and the way that over-compliance is reflected in the enforcement strategy, yet this spirit of collaboration at times finds itself at odds with the formal regime.

To follow up on the ***regulatory regime and style***, the regulatory regime will have to allow for systems-based supervision to enable the benefits. Whether such supervision regime is possible depends on the data (transaction data, output data, meta data on the organisation) that is available and the extent to which supervisors depend on that kind of data of the regulated. Furthermore, as over-compliance is often new and sometimes restricted to the 'best in class', the style of the supervisor is often based on collaboration. This means that the supervisor will coach the company towards a situation that they are both happy with. This is also an intensive phase; although actual supervision for that company will over time take less resources, setting everything up, takes up more. The question is for what number of companies that can be done and what that would require of auditors. It also depends on the specific sector. For example, are there professional incentives for self-regulation?

Finally, ***context-awareness*** is an issue, especially for sensitive data. The new possibilities to process large amounts of data (e.g. data mining) make it harder to protect sensitive data. A data element is not necessarily sensitive in and by itself, but may become that when aggregated or combined with other data elements. It is challenging to keep track of which combinations are sensitive and who has (had) access to what data in case there are many parties involved, or there are large volumes of data with many different elements. To still protect sensitive data, the juridical and technical safeguards need to be aligned. That depends on the motives of both the regulated and the supervisor, but also on the institutional context and supervision regime.

Being aware of the context in which information is created and/or shared, is important for assessing the compliance of those companies. With the abundance of information available today, there are more data and meta-data available to feed (latent) variables that measure compliance. However, this situation also leads to new challenges and questions; for example on regulatory options for taking into account context as meta-data. Furthermore, if information sharing systems themselves become more context aware, how to know what is not being shared, what is altered and what is only valuable for a specific context? What is the role and value of internal control in those situations, and what does this mean for IT auditors? If information is not shared; how can government agencies know whether that is for good contextual reasons or when that is because of unwillingness to share? How can you know what information is being withheld, and assess whether that means something for establishing compliance or providing the benefits associated with over-compliant information sharing?

Although recently studies have started to cover the technical challenges of such context-aware information sharing [38], what that means in terms of the supervision relationship, has not yet been explored. This is an important research direction, as for the further development of context-aware, over-compliant information sharing, it is vital that the supervision implications of sharing decisions are known.

5 Conclusions

In this paper we have looked at three R&D projects to extract lessons on the implications that over-compliant B2G information sharing may have on the relationship between regulatory supervision and the regulated. In the cases we find that there are many variables and complexities that play a role in that relationship which are affected by the technical innovation. The work on the technical innovations tends not to focus too much on those. Especially regulatory benefits are easily counted on as a key incentive for companies to change the relationship with the supervisor into a much more collaborative one, in which they can share additional data in return for compliance benefits. However, as this is a field where the technical innovation meets soft variables, the effects of the innovation on the relationship and vice versa may not be so clear-cut. Apart from the known issues in public-private collaboration (e.g. control, autonomy, amoral behaviour, conflicting goals and interests), even collaborations that are genuinely committed to making over-compliant B2G information sharing work for both sides encounter push-back from the economic rationality for the company and the institutional and regulatory environment of the supervision regime. A changing relationship between regulator, supervisor, and the regulated, especially when enabled by data, will have to start from certain anticipation effects, such as trust and expectations. Yet, the challenges that we found in this paper (although probably only a small portion of all those out there) show that the institutionalisation of the previous relationship when combined with uncertainties of how new technologies will play out, make the process much more cumbersome than most parties set out with.

The three projects covered in this paper have led to new supervision relationships, but only for a handful of companies and also government agencies are finding it hard to scale up. That is not strange, as even in face of great benefits, the new challenges are equally great. We have institutionalised so much value in the current supervision regimes, that we are only beginning to find out how to address things like internal control, external audits, control frameworks, discretionary freedoms, strategic selection, and many others have to be adapted to ever more data.

References

1. Bharosa, N., et al.: Tapping into existing information flows: the transformation to compliance by design in business-to-government information exchange. Gov. Inf. Q. **30**, 9–18 (2013)
2. Bharosa, N., van Wijk, R., de Winne, N., Janssen, M.: Challenging the Chain: Governing the Automated Exchange and Processing of Business Information. IOS Press, Amsterdam (2015)

3. van der Pligt-Benito Ruano, S., Hulstijn, J.: Governance and collaboration in regulatory supervision: a case in the customs domain. Int. J. Electron. Gov. Res. **13**, 34–52 (2017)
4. Veenstra, A.W., Hulstijn, J., Christiaanse, R., Tan, Y.-H.: Information exchange in global logistics chains: an application for model-based auditing (2013)
5. Tan, Y.-H., Bjørn-Andersen, N., Klein, S., Rukanova, B.: Accelerating Global Supply Chains with IT-Innovation. ITAIDE Tools and Methods. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-15669-4
6. Klievink, B., Bharosa, N., Tan, Y.-H.: The collaborative realization of public values and business goals: governance and infrastructure of public–private information platforms. Gov. Inf. Q. **33**, 67–79 (2016)
7. Van Veenstra, A.F.: IT-Induced Public Sector Transformation (2012)
8. Urciuoli, L., Hintsa, J., Ahokas, J.: Drivers and barriers affecting usage of e-customs — a global survey with customs administrations using multivariate analysis techniques. Gov. Inf. Q. **30**, 473–485 (2013)
9. Gil-garcia, J.R., Chengalur-Smith, I., Duchessi, P.: Collaborative e-government: impediments and benefits of information-sharing projects in the public sector. Eur. J. Inf. Syst. **16**, 121–133 (2007)
10. Robey, D., Im, G., Wareham, J.D.: Theoretical foundations of empirical research on interorganizational systems: assessing past contributions and guiding future directions. J. Assoc. Inf. Syst. **9**, 497–518 (2008)
11. Hart, P., Saunders, C.: Power and trust: critical factors in the adoption and use of electronic data interchange. Organ. Sci. **8**, 23–42 (1997)
12. Klievink, B., Lucassen, I.: Facilitating adoption of international information infrastructures: a living labs approach. In: Wimmer, M.A., Janssen, M., Scholl, H.J. (eds.) EGOV 2013. LNCS, vol. 8074, pp. 250–261. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40358-3_21
13. Zuidwijk, R.A., Veenstra, A.W.: The value of information in container transport. Transp. Sci. **49**, 675–685 (2015)
14. Bharosa, N., Janssen, M., Hulstijn, J., van Wijk, R., de Winne, N., Tan, Y.: Towards a lean-government using new IT-architectures for compliance monitoring. In: Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance - ICEGOV 2011, p. 147 (2011)
15. Kagan, R.A., Scholz, J.: The criminology of the corporation and regulatory enforcement strategies. In: Blankenburg, E., Lenk, K. (eds.) Organisation und Recht. Jahrbuch für Rechtssoziologie und Rechtstheorie, vol. 7, pp. 352–357. Springer, Heidelberg (1980). https://doi.org/10.1007/978-3-322-83669-4_21
16. Hawkins, K.: Environment and Enforcement, Regulation and the Social Definition of Pollution. Clarendon Press, Oxford (1984)
17. Braithwaite, J.: To Punish or Persuade: Enforcement of Coal Mine Safety (1985)
18. Sparrow, M.: The Regulatory Craft: Controlling Risks, Solving Problems, and Managing Compliance (2011)
19. van Wingerde, K.: The limits of environmental regulation in the global economy. In: van Erp, J., Huisman, W., Vandewalle, G. (eds.) The Routledge Handbook of White-Collar and Corporate Crime in Europe, pp. 260–275. Routledge, London (2015)
20. Reiss, A.: Consequences of compliance and deterrence models of law enforcement for the exercise of police discretion. Law Contemp. Probl. **47**, 83 (1984)
21. de Bruijn, H., ten Heuvelhof, E., Koopmans, M.: Law Enforcement: The Game Between Inspectors and Inspectees (2007)
22. Ayres, I., Braithwaite, J.: Responsive Regulation: Transcending the Deregulation Debate (1992)

23. Six, F.E., Verhoest, K.: Trust in regulatory regimes; scoping the field. In: Six, F.E., Verhoest, K. (eds.) Trust in Regulatory Regimes, pp. 1–36. Edward Elgar, Cheltenham (2017)
24. Van Der Voort, H.: Trust and cooperation over the public-private divide. In: Six, F.E., Verhoest, K. (eds.) Trust in Regulatory Regimes, pp. 181–204. Edward Elgar, Cheltenham (2017)
25. May, P.: Regulatory regimes and accountability. Regul. Gov. **1**, 8 (2007)
26. Coglianese, C.: Management-based regulation: prescribing private management to achieve public goals. Law Soc. Rev. **37**, 691 (2003)
27. Gunningham, N., Grabosky, P., Sinclair, D.: Smart Regulation: Designing Environmental Policy (1998)
28. Black, J.: Decentring regulation: understanding the role of regulation and self-regulation in a "post-regulatory" world. Curr. Leg. Probl. **54**, 103 (2001)
29. Haines, F.: The Paradox of Regulation: What Regulation Can Achieve and What It Cannot (2011)
30. Garcia Martinez, M., Verbruggen, P., Fearne, A.: Risk-based approaches to food safety regulation: what role for co-regulation? J. Risk Res. **16**, 1101 (2013)
31. Baldwin, R., Black, J.: Really responsive regulation. Mod. Law Rev. **71**, 59 (2008)
32. Black, J., Baldwin, R.: Really responsive risk-based regulation. Law Policy **32**, 181 (2010)
33. Van der Voort, H., Kerpershoek, E.: Measuring measures: introducing performance measurement in the Dutch health care sector. Pub. Money Manag. **30**, 63–68 (2010)
34. Klievink, B., et al.: Enhancing visibility in international supply chains: the data pipeline concept. Int. J. Electron. Gov. Res. **8**, 14–33 (2012)
35. Van Engelenburg, S., Janssen, M., Klievink, B.: Design of a software architecture supporting business-to-government information sharing to improve public safety and security: combining business rules, events and blockchain technology. J. Intell. Inf. Syst. 1–24 (2017). https://doi.org/10.1007/s10844-017-0478-z
36. Hesketh, D.: Weaknesses in the supply chain: who packed the box? World Cust. J. **4**, 3–20 (2010)
37. Baida, Z., Rukanova, B., Liu, J., Tan, Y.: Preserving control in trade procedure redesign – the beer living lab. Electron. Mark. **18**, 53–64 (2008)
38. van Engelenburg, S., Janssen, M., Klievink, B.: What belongs to context? In: Cerone, A., Roveri, M. (eds.) SEFM 2017. LNCS, vol. 10729, pp. 101–116. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-74781-1_8