Technologies of Compliance: Risk and Regulation in a Digital Age

Kenneth A. Bamberger
Legal scholarship has been silent about a phenomenon with profound implications for governance: the automation of compliance with laws mandating risk management. Regulations—from bank capitalization rules, to Sarbanes-Oxley's provisions on financial fraud and misrepresentation, to laws governing information-privacy protection—frequently require regulated firms to develop internal processes to identify, assess, and mitigate risk. To comply, firms have turned wholesale to technology systems and computational analytics that measure and predict corporate risk levels and "force" decisions accordingly. In total, the third-party market for compliance-technology products—known generally as "governance, risk, and compliance" (GRC) software, systems, and services—alone grew to $52 billion last year, and this growth is poised to increase exponentially.

While these technology systems offer powerful compliance tools, they also pose real perils. They permit computer programmers to interpret legal
requirements; they mask the uncertainty of the very hazards with which policy makers are concerned; they skew decisionmaking through an “automation bias” that privileges personal self-interest over sound judgment; and their lack of transparency thwarts oversight and accountability. These phenomena played a critical role in the recent financial crisis.

This Article explores these developments and the failure of risk regulation to address them. While regulators have lauded the turn to technology, they have ignored its perils. By contrast, this Article investigates the accountability challenges posed by these and other technologies of control, and suggests specific reform measures for policy makers revisiting the governance of risk. This Article argues for more activist regulator oversight backed by sanctions before disaster has occurred. But it also emphasizes collaboration in developing risk-management systems, drawing both on the granular expertise of firms and the broader vantage of administrative agencies. Most importantly, it seeks better to reflect the human decisionmaking element at both levels: to recognize the ways in which technology can hinder good judgment, to reintroduce human inputs in the decision process, and to reflect the limits of both human and computer reasoning.

I. Introduction

II. Regulatory Delegation and the Procedural Regulation of Risk

III. The Turn to Technology, and Its Benefits
   A. Technology’s Efficiencies
   B. Technology’s Effectiveness
      1. The IT Toolbox
      2. GRC Systems
         a. Identification and Measurement of Key Risks
         b. “Forcing” Compliance Through Controls
         c. Monitoring Risk Management
            i. Automating the Audit Function
            ii. Centralizing Risk Oversight
            iii. Real-Time Decision Support for Risk Mitigation
         d. Compliance with Reporting Requirements

IV. Technology Pitfalls and the Challenge for Governance
   A. The Reticent Regulator
   B. The Perils of Technology
      1. Problems of Translation
      2. Systemic Effects
      3. Cognitive Bias in Decisionmaking
      4. Opportunities for Gamesmanship
   C. Technology Pitfalls on the Ground: Illustrative Cases
      1. Case 1: Technology Limits and Information Privacy
      2. Case 2: Technology Failures and the Financial Crisis
In December 2006, executives at financial-services firm Goldman Sachs quickly convened a meeting of senior risk managers and traders. After three hours examining the breadth of its trading positions, the firm decided to limit exposure to a housing-market downturn by selling some of its mortgage-backed securities and diversifying its holdings to hedge the risk of others. While Goldman suffered losses in 2007, they reached nowhere near the scale of those suffered by its contemporaries. The firm avoided the fate of now-defunct competitors such as Bear Stearns, Lehman Brothers, and Merrill Lynch, and went on to earn record profits in 2009.

The meeting’s fortuitous timing was no coincidence. Since the 1980s, Goldman had invested heavily in risk-modeling technology. Unlike some of its competitors, Goldman’s system had incorporated into its monitoring capacity daily trend reporting based on sophisticated, quantitative risk-prediction programs. In December 2006, Goldman’s system indicated a

2. The firm even alleges that if insurer AIG had been allowed to fail in September 2008, Goldman would not have been hurt despite the fact that it held $13.98 billion in collateralized debt obligations written by AIG. See Peter Eavis, Goldman’s Price of Protection, WALL ST. J., Mar. 18, 2009, at C14 (“If Goldman were able to withstand the bankruptcy of a large counterparty like AIG without material hits, it would bolster the view that Goldman is a savvy risk manager, and that its stock deserves to trade at a premium to other banks to reflect that.”).
3. See infra note 41.
5. See Editorial, On Top of the World: Goldman Sachs, ECONOMIST, Apr. 29, 2006, at 11 (chronicling that Goldman built a “proprietary technology system” that was “unmatched at rivals”).
6. See Nina Mehta, FEN One on One Interview with Emanuel Derman, FINANCIAL ENGINEERING NEWS, July/Aug. 2003, http://www.ederman.com/new/docs/fen-interview.html. In this interview, former Goldman risk modeler Emanuel Derman observed:
problem—the firm’s daily profit and loss reports showed that its mortgage business had posted a loss for ten straight days. The generation of those ten daily reports triggered the meeting, and the evaluation of firm-wide exposure measures generated by its risk-assessment technologies, in turn, prompted the subsequent realignment.

Goldman’s experience underscores a phenomenon about which legal scholarship has been remarkably quiet: the increasingly pervasive reliance on technology—in the form of information-technology and decision-automation system software and analytics—in assessing and controlling risk, and in complying with government regulation mandating its management. This development has particularly marked compliance with legal regimes that require firms themselves to develop internal controls to identify, assess, and mitigate risk. Such regimes include banking regulation governing the capitalization of financial institutions, the Sarbanes-Oxley Act’s provisions targeting financial fraud and misrepresentation, and laws governing information-privacy protection.

These regimes typify a new model of regulation. This “process-based” or “management-based” model responds to the combination of

In a good way, Goldman Sachs was eclectically irreverent about what was the right way to look at risk. We didn’t just rely on VAR. Estimates of the probability of bad things happening are notoriously poor because crises don’t repeat themselves in exactly the same way. We relied on scenario analysis and stress-testing as well. There were limits on positions, for instance, in order to limit the loss that would occur under a repeat of the 1998 country-default scenario.

Id.

7. Nocera, supra note 1, at 27.
8. Id.
9. See generally Paul N. Otto & Annie I. Antón, Managing Legal Texts in Requirements Engineering, in DESIGN REQUIREMENTS ENGINEERING: A TEN-YEAR PERSPECTIVE 374, 374 (K. Lyytinen et al. eds., 2009) (“Requirements for software systems are increasingly originating in laws and regulations.”).
10. See, e.g., 12 U.S.C. § 281 (2006) (requiring that any bank within the Federal Reserve system have “subscribed capital” of at least $4 million); id. § 461(b)(2)(A) (mandating that banks maintain a percentage of reserves as determined by the Federal Reserve Board of Governors); infra notes 64–67 and accompanying text.
challenges that often make risk regulation difficult. Risk is contextual and manifests itself differently across heterogeneous firms.\textsuperscript{15} Regulated firms have far better information than the agencies who oversee them regarding firm organization as well as the sources of risk and capacity for risk mitigation.\textsuperscript{16} Moreover, risk is difficult to assess—even from an insider vantage. Thus, risk regulation often cannot be boiled down to either “command-and-control” behavioral mandates or to the type of uniform rules that set particular measurable outcomes, such as those prevalent in much of environmental regulation.

Modern risk regulation, therefore, takes a different tack, eschewing mandated outcomes and requiring instead that regulated firms develop individualized, internal risk-management \textit{processes}. Such regulation identifies risk-mitigation goals generally—such as “managing the risks associated with” the over-the-counter derivatives trade.\textsuperscript{17} But it ultimately enlists the judgment of regulated firms themselves, delegating to them the tasks of interpreting the regulatory norm in local context and implementing the appropriate response. In these contexts, implementation by private institutions ultimately animates the law’s meaning.

In response to such requirements, regulated firms have turned to technology. More specifically, they have both adapted existing information-technology systems developed in the first instance for private management purposes and developed new ones intended specifically to satisfy government mandates. Given the scale and complexity of contemporary business institutions and the massive amount of information involved in corporate operations, the types of risk controls that regulation demands simply cannot function without the data collection, analyzing, and monitoring capacities of integrated computer technology.\textsuperscript{18} Government regulators thus urge compliance through “increasing standardization and automation”\textsuperscript{19} and the

\begin{footnotesize}
\begin{enumerate}
\item[15.] Bamberger, supra note 13, at 380.
\item[16.] See Coglianese \& Lazer, supra note 14, at 695 (asserting that a management-based approach is preferable to a traditional government-imposed regulatory standard because it “place[s] responsibility for decisionmaking with those who possess the most information about risks and potential control methods”).
\item[17.] See 17 C.F.R. § 240.15c3–4(a) (2009) (“An OTC derivatives dealer shall establish, document, and maintain a system of internal risk management controls to assist it in managing the risks associated with its business activities, including market, credit, leverage, liquidity, legal, and operational risks.”).
\end{enumerate}
\end{footnotesize}
use of “forensic tests and new technology.”

Third-party software vendors offer fully-automated risk analytics and controls. Influential consulting firms and auditors further contribute: IBM Corporation promotes a “Unified Governance Framework” based on extensive software research into REALM (REgulations As Logical Models); Deloitte LLP studies document the economies gained by automating risk-management controls; and one Ernst & Young LLP partner concludes simply, “The more controls a company can move from manual to automated, the better.”

In total, the third-party market for compliance-technology products is big and getting bigger. The total market for “governance, risk and compliance” (GRC) software, systems, and services was estimated at $52 billion in 2008, with around $9 billion of that coming directly from GRC technology providers. This growth, moreover, is poised to increase exponentially as the U.S. Congress and the Obama Administration have proposed significant expansion of risk-management requirements in a host of previously unregulated contexts.

GRC systems, indeed, offer powerful compliance tools. They typically automate the integration and analysis of huge amounts of data, inform high-level decisionmakers regarding levels and locations of risk, and “force” con-
sequent decisions through rules that shape and limit the discretion that can be exercised by individuals within firms. Through such automation, they can provide powerful information security, accuracy, and privacy architectures; prevent employee fraud and malfeasance; audit transactions for compliance; and monitor—in near real time—risk measures that trigger regulatory requirements, like loss reporting or increases in capital reserves.

Yet these same compliance tools can also pose catastrophic dangers. As this Article describes, reliance on the very same types of risk-management technologies that "saved" Goldman played a critical role in failures at the heart of the broader financial crisis. Risk-assessment analytics, premised on unrealistic assumptions, diverged increasingly from accurate market representations. At the same time, automated systems—systems that governed loan originations, measured institutional risk, prompted investment decisions, and calculated capital-reserve levels—shielded irresponsible decisions, unreasonably risky speculation, and intentional manipulation with a façade of regularity. In the words of former Federal Reserve Chairman Alan Greenspan, the "whole intellectual edifice" of the "modern risk management paradigm"—a paradigm relying on mathematical and financial insights "supported by major advances in computer and communications technology"—has "collapsed."

With these experiences in mind, this Article explores the pervasive use of technology to automate risk-management compliance and considers its consequences. While these developments have drawn scant remark in the legal literature, they have broad implications for governance. If delegating to private firms the broad authority to develop their own risk-management controls allows those firms to fill out the meaning of legal norms, then the technology used in this process (and its underlying analytics and metrics) generates that meaning. "Code," in the words of information-technology scholars, really is constitutive of "law."

Yet the use of technology systems to hardwire compliance raises fundamental issues regarding the translation of legal mandates. Technology is not neutral; the reduction of regulation to code embodies particular choices

27. See Mary Hayes Weier, Comply or Die: GRC Software Ain't Sexy, but It Sure Sells, INFORMATIONWEEK, Apr. 7, 2008, at 28, 28 (noting the widespread adoption of GRC software and discussing specific examples of executive reporting and workflow management features).
28. See id. (describing use of GRC software for both security and compliance goals including fraud prevention, internal data integrity, auditing, and compliance reporting).
29. See infra section IV(C)(2).
as to how the law is interpreted. Those choices may be shaped by a variety of extralegal factors, including the conscious and unconscious professional assumptions of programmers and "quants" (economists, physicists, and mathematicians), as well as bottom-line business incentives. Those choices, in turn, may be embedded in a way that is difficult to identify or alter as contexts change.

Technology, then, is shaped by a system of logic distinct from either law or management. Technology-based compliance systems have proliferated specifically in contexts in which legislators and policy makers have rejected rule-based mandates in favor of context-specific judgment by regulated entities. Computer code, by contrast, operates by means of on-off rules, while the analytics it employs seek "to quantify the immeasurable with great precision."

Because of these attributes, technology systems are not merely tools for implementing the goals of those who employ them; they shape the meaning of those goals themselves. In Heidegger's words, they create a Gestell, or world view, that alters the perceptions of the decisionmakers they inform. In the context of risk, they privilege the measurable and mask uncertainty, obscuring the very hazards with which policy makers are concerned and clouding the judgment of users upon whom risk regulation relies. Moreover, they create automation biases—decision pathologies that hinder careful review of automated outcomes, especially by those with financial incentives that promote risky behavior. These very phenomena contributed to the failure of risk regulation and risk management to prevent the recent financial meltdown.

Additionally, technology frequently lacks transparency, creating an additional layer of obscurity for those seeking to monitor business operations and compliance inside and outside the firm. By technology's operation—the perfect way in which its rule-based systems exclude some factors and include others—it can render the choices and metrics embedded in compliance systems by private third parties invisible to regulators. These developments, in turn, raise what might be called administrative-law concerns—concerns regarding the subversion of public norms requiring transparency, public oversight, and accountability in the exercise of regulatory discretion.

This Article proceeds by exploring these phenomena and risk regulation's failure to address them. Parts II and III describe prevailing management-based or process-based approaches to risk regulation as well as

32. See Hiroyuki Itami & Tsuyoshi Numagami, Dynamic Interaction Between Strategy and Technology, 13 STRATEGIC MGMT. J. 119, 129 (1992) (distinguishing technology from science and bureaucracy by describing technology as "a set of knowledge and beliefs on causal relations and thus a system of logic").


the inevitable push towards technology systems as a means for compliance with legal and managerial requirements for risk management.

Part IV describes the "perils" of technological compliance—the ways in which technology systems intended to manage risk can mask both uncertainty and malfeasance, thus creating different types of risk—and the central role of such shortcomings in accelerating the current financial crisis. These characteristics of compliance technology can both damage regulation's effectiveness and undermine important public-law norms regarding the accountable exercise of regulatory discretion.

Part V addresses these implications for governance and explores policy approaches for policy makers revisiting the regulation of both firm-specific and systemic risk. Drawing on experiences with "technologies of control" in other contexts, this Part categorizes various accountability concerns raised by such tools and a variety of solutions proposed to address them. It then identifies which might have particular salience in the compliance setting.

Specifically, it argues for a more activist regulatory model that exploits, rather than ignores, technology's boundary-spanning potential as a means for enhancing transparency in two directions. On the one hand, technology can provide regulators and third parties entrusted with market oversight significantly enhanced access to the workings of organizational decisionmaking, and can thus serve as a mechanism for making firms into better regulatory targets. On the other, more sustained regulator participation in the development of risk-analysis technology can offer better guidance as to regulator preferences, promoting effective policy, important rule-of-law values, and greater accountability.

This model relies on much more intense regulator involvement in requiring transparency, structuring firm decision processes, measuring the effectiveness of internal controls, and providing the possibility for sanctions before catastrophic failure has occurred. But it also emphasizes collaboration in the process of developing risk-management systems, drawing both on the granular expertise of firms and on the broader vantage of the administrative agency. Perhaps most importantly, it seeks to better reflect the human decisionmaking element at both levels: to recognize the ways in which technology can constrain that element, to reintroduce human judgment in the decision process, and to reflect the limits of both human and computer reasoning.

II. Regulatory Delegation and the Procedural Regulation of Risk

The risks generated by individual firm operations create significant social costs. The inaccurate assessment of the risks associated with existing as a business, or risk taken on with the purpose of calculated reward—such as market or capital risk—can externalize significant costs on consumers,
investors, and other market players. Moreover, the failure to address synthetically the ways in which the risk of any individual enterprise is interdependent with industry risk generally can threaten systemic effects of the type implicated in the ongoing financial meltdown.

Yet regulating the financial and operational risks of private-market activity is notoriously difficult. Organizational structures, areas of business focus, and operational procedures within individual firms are heterogeneous. Furthermore, risk arises from the interplay of a variety of different factors, and its manifestations diverge by context. Risk’s regulation, therefore, often cannot be boiled down to traditional regulatory forms—uniform ex ante rules mandating either specific behaviors or particular measurable outcomes. Regulators, moreover, lack a clear vantage point for identifying either threats on the ground or private information about firm organization necessary for developing top-down requirements of risk-mitigating behavior.

At the same time, the public interest in mitigating risk ex ante, rather than after harm has occurred, is clear. While, for example, numerous regulatory enforcement actions and private legal suits have been brought against banks and other financial institutions in the past months for conduct contributing to the systemic financial crisis, much of the damage is irreversible. Such ex post legal measures can often do little to either undo the resulting social harm or provide requisite restitution—due in no small part to the fact that many of the targeted institutions have ceased to exist.

35. See Viral V. Acharya et al., The Financial Crisis of 2007–2009: Causes and Remedies, in RESTORING FINANCIAL STABILITY: HOW TO REPAIR A FAILED SYSTEM 1, 24–25 (Viral V. Acharya & Matthew Richardson eds., 2009) (“[T]he firm has no specific incentive to consider the spillover risk its own leverage and risk taking imposes on other financial institutions. This externality is further amplified when many of the financial firms face similar issues.”).

36. See Appelbaum & Cho, supra note 26 (explaining that Geithner’s plan will limit the risk taking at individual firms in order to avoid setting off cascading damage).

37. See EUGENE BARDACH & ROBERT A. KAGAN, GOING BY THE BOOK: THE PROBLEM OF REGULATORY UNREASONABLENESS 58–66 (discussing the difficulty of regulating among firms that have diverse manufacturing technologies and procedures, varied nonlegal incentives to comply with regulations, and disparate organizational and managerial capacities to ensure that compliance).

38. Bamberger, supra note 13, at 380.

39. See Edward L. Rubin, Images of Organizations and Consequences of Regulation, 6 THEORETICAL INQUIRIES L. 347, 386 (2005) (describing the assumption behind many incentive-based approaches to regulation that regulators impose counterproductive measures because they lack knowledge of particular firms’ internal operations).

40. See, e.g., Lawyerlinks.com, Credit Crunch: Company Roll-Up, http://content.lawyerlinks.com/sec/Liability/credit_crunch/1_roll_up/2_companies.htm#Litigation (listing, and linking to materials from, dozens of securities and derivative suits brought against the “Credit Crunch” “Big Targets”).

41. See, e.g., FED. RESERVE BANK OF N.Y., FINANCIAL TURMOIL TIMELINE 4–5 (2010), http://www.ny.frb.org/research/global_economy/Crisis_Timeline.pdf (chronicling the purchase of Bear Stearns by JP Morgan Chase, the bankruptcy of Lehman Brothers, the purchase of Merrill Lynch by Bank of America, the seizure and receivership of Washington Mutual, and the purchase of Wachovia by Wells Fargo).
This regulatory challenge reflects, to a large extent, the sociological insights of systems theory. These insights highlight the difficulty faced by one system (here, law), which derives its legitimacy from a certain self-contained set of practices, in prescribing behavior that will lead to particular outcomes in another system (business or economics), which is governed by a different—or even incommensurate—rationality. This account, in turn, suggests a "new" approach to governance. When a social problem eludes both traditional ex ante and ex post solutions—when, in economic terms, the regulated agent is relatively insensitive to top-down commands from regulator principals—then regulators might have greatest influence in steering the decisions of a variety of organizational players towards policy principles rather than trying to dictate the outcomes.

Consistent with these insights, regulatory efforts at curbing risk itself have largely focused on regulating risk management. Such management-based or process-based regulation articulates public goals and requires regulated firms to develop internal processes and controls geared towards their achievement. Yet it delegates, to regulated entities themselves, wide discretion in deciding how to interpret and achieve those goals in particular contexts. Such regulatory delegation thus enlists the judgment of firm decisionmakers to draw on the superior knowledge of internal firm workings that are inaccessible to regulators, and seeks to harness firm risk-management systems as regulatory assets by aligning public and private incentives.

Section 404 of the Sarbanes–Oxley Act is perhaps the most well-known example of a management-based regulatory regime: it requires the development of internal risk-management systems quite broadly. By its mandate, all publicly traded companies must develop internal controls for assuring the

---

42. See Niklas Luhmann, The Unity of the Legal System, in AUTOPOIETIC LAW: A NEW APPROACH TO LAW AND SOCIETY 12, 27 (Gunther Teubner ed., 1987) (observing that the legal system is a "normatively closed but cognitively open system" that must take into account the "normative expectations" of systems outside the law). For an account that emphasizes the demise of state-centered regulation, see Philip G. Cerny, Embedding Global Financial Markets: Securitization and the Emerging Web of Governance, in PRIVATE ORGANIZATIONS IN GLOBAL POLITICS 59, 67–68 (Karsten Ronit & Volker Schneider eds., 2000).

43. See Orly Lobel, The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought, 89 MINN. L. REV. 342, 342–50 (2004) (describing the recent shift from the traditional "New Deal" regulatory era to a "Renew Deal" governance paradigm in which government, industry, and society "share responsibility for achieving policy goals").

44. See, e.g., id. at 357–58 (describing arguments that the traditional regulatory state can no longer keep up with a society that is increasingly complex, unpredictable, and volatile).

45. See Coglianese & Lazer, supra note 14, at 696–700 (describing the use of management-based regulation in the areas of food safety, industrial safety, and pollution prevention).

46. Id. at 695–96.

accuracy of financial reports and disclosures. The administrative guidance implementing Sarbanes–Oxley requires that firms evaluate specific control elements, yet it leaves firm management wide discretion in its assessment approach.

In a variety of contexts, moreover, regulatory delegation has become the mechanism of choice for governing risk. Two specific contexts, which are considered later in subpart IV(C) as “case studies,” are (1) the regulation of information privacy across sectors and (2) the more targeted regulation of risk in financial institutions.

As to the first, firms in a variety of sectors that possess different types of personally identifiable information must establish risk-assessment and data-security systems to protect its privacy and security. The regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA), for example, require regulated health-care entities to implement systems that protect the confidentiality of electronic health information in their possession, identify confidentiality risks, contain security measures “sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level,” and ensure compliance by employees.

The Federal Trade Commission’s 2003 standard—which implements Title V of the Gramm–Leach–Bliley Act (GLBA)—similarly empowers

---

49. See, e.g., BYLAWS AND RULES, Auditing Standard No. 5, § A5 (Pub. Accounting Oversight Bd. 2007), available at http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf (defining “internal control over financial reporting” as a process designed by, or under the supervision of, the principal executives or financial officers of a company to provide reasonable assurance regarding the maintenance of adequate accounting records and the prevention of unauthorized acquisition, use, or disposition of the company’s assets). Procedure-based mandates, moreover, arise from a combination of public and private sources. The enterprise risk-management framework was developed by the private-sector Committee of Sponsoring Organizations of the Treadway Commission (COSO). COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM’N, ENTERPRISE RISK MANAGEMENT—INTEGRATED FRAMEWORK, at v (2004), available at http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf [hereinafter COSO]. This framework, which has largely guided individual firms’ compliance approach to Sarbanes–Oxley and other regulations mandating internal controls, provides important guidance regarding the required elements of a risk-management program and its auditing. The enumerated elements include appropriate risk assessment, institutional risk responses, and control activities. Id. at 3–4. Nevertheless, the framework leaves much of the implementation detail open to context. The New York Stock Exchange listing standards require Board Audit Committees to “discuss guidelines and policies to govern the process” for risk assessment and risk management. NYSE, Listed Company Manual § 303A.07(c)(iii)(D) (2009).
52. Id. § 164.308(a)(1)(ii)(A).
53. Id. § 164.308(a)(1)(ii)(B).
54. Id. § 164.306(a)(4).
various agencies to promulgate data-security regulations for financial institutions.\textsuperscript{56} In turn, the standard instructs firms to develop risk-assessment and data-security systems “appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.”\textsuperscript{57} While the implementing regulations do include some guidance for implementation tools, such as “periodic risk assessments” and “sanctions against employees that fail to comply,” the particularized implementation is left to individual firms, and “[t]he ultimate test remains a broad one, that of ‘reasonable data security.’”\textsuperscript{58} Moreover, the proposed Personal Data Privacy and Security Act of 2009,\textsuperscript{59} reported out of Senate committee in November 2009, would similarly require all firms to “implement a comprehensive personal data privacy and security program that includes [appropriate] administrative, technical, and physical safeguards” to identify, manage, and control the risk of privacy breaches.\textsuperscript{60}

This approach dominates the regulation of financial institutions as well. Regulation governing the “safety and soundness” of banks, for example, relies largely on process-based regulation.\textsuperscript{61} It requires banks to develop “internal controls and information systems that are appropriate to the size of the institution and the nature, scope and risk of its activities” that provide for effective risk management, adequate safeguards for asset management, legal compliance, structures and systems geared to internal monitoring and audits, and accurate reporting.\textsuperscript{62} Moreover, banks must maintain a system to identify problem assets and prevent their deterioration. Such a system should involve periodic asset-quality reviews; estimations of losses and the establishment of sufficient reserves to absorb them; and consideration of the “size and potential risks of material asset concentrations.”\textsuperscript{63}

The Basel II banking-regulation regime similarly relies on internal processes to derive bank capital-adequacy requirements in light of credit, operational, and market risks.\textsuperscript{64} Specifically, the international accord permits

\textsuperscript{56} 15 U.S.C. §§ 6801, 6805.
\textsuperscript{57} 16 C.F.R. § 314.3(a) (2009).
\textsuperscript{60} Id. § 302(a)(1)–(3).
\textsuperscript{62} Id. § II(A).
\textsuperscript{63} Id. § II(G).
\textsuperscript{64} See DIMITRIS N. CHORAFAS, OPERATIONAL RISK CONTROL WITH BASEL II 117 (2004) (noting that the capital requirements include market, operational, and credit risk exposures). The international Basel II Accord embodies recommendations on banking regulation developed by the Central Bank Governors of the Group of Ten nations through the Basel Committee on Banking
national regulators to allow large institutions to opt out of standard capital requirements if they use internal risk models that meet certain standards.65 The joint guidance promulgated by U.S. bank regulators pursuant to that framework articulates specific factors that must be incorporated into a bank’s internal risk-assessment procedures,66 but ultimately “[t]he qualification requirements for these systems are written in broad terms to accommodate the many ways a bank may design and implement a robust internal risk measurement and management system and to permit industry practice to evolve.”67

Other regimes governing financial institutions require banks to establish internal controls furthering compliance with the USA PATRIOT Act, the Bank Secrecy Act, and other anti-money-laundering requirements.68 They require investment advisers to adopt policies and procedures “reasonably designed to ensure that [the adviser] vote[s] . . . in the best interest of clients.”69 And they require derivatives dealers to “maintain a system of


65. See BASEL COMM. ON BANKING SUPERVISION, INTERNATIONAL CONVERGENCE OF CAPITAL MEASUREMENT AND CAPITAL STANDARDS: A REVISED FRAMEWORK 1990 (2006) [hereinafter BASEL, A REVISED FRAMEWORK], available at http://www.bis.org/publ/bcbs128b.pdf (“Where a bank has a VaR measure that incorporates specific risk and that meets all the qualitative and quantitative requirements for general risk models, it may base its [specific risk capital] charge on modeled estimates . . . “).  

66. The final guidance issued after notice and comment on July 16, 2008 by the Federal Reserve Board, the FDIC, the OCC, and the Office of Thrift Supervision. It outlined the implementation of Basel II, for example, stating that in measuring credit risk,

The bank should consider the various types of dependence among exposures, and the credit risk effects of extreme outcomes, stress events, and shocks to assumptions about portfolio and exposure behavior. The bank also should carefully assess concentrations in counterparty credit exposures, including those that result from trading in less liquid markets, and determine the effect that these exposures might have on capital adequacy. Supervisory Guidance: Supervisory Review Process of Capital Adequacy (Pillar 2) Related to the Implementation of the Basel II Advanced Capital Framework, 73 Fed. Reg. 44620, 44625 (July 31, 2008) (to be codified at 12 C.F.R. pts. 3, 208, 325, 3567). Similarly, any determination of market risk should consider a variety of factors:

illiquidity of instruments, leverage, concentrated positions, one-way markets, nonlinear or deep out-of-the-money option positions as well as embedded optionality, and the potential for significant shifts in correlations or other types of dependence structures. Assessments that incorporate extreme events, idiosyncratic variations, credit migrations or changes in credit spreads, defaults, and shocks should also be tailored to capture key portfolio vulnerabilities.

Id.


internal risk management controls to assist it in managing the risks associated with its business activities, including market, credit, leverage, liquidity, legal, and operational risks.” ⁷⁰

The multiplicity of management-based requirements is only set to spiral upwards. In the wake of the financial crisis, Congress and the Obama Administration have both proposed significant expansions of risk-management oversight in previously unregulated contexts. ⁷¹ Ratings agencies have begun to include assessment of a firm’s enterprise risk-management procedures in their credit ratings of both financial and non-financial companies. ⁷² Moreover, increasing scrutiny of insurers, AIG among them, has increased pressure on U.S. regulators to adopt international regimes like Solvency II, the Basel II-like risk-assessment framework already adopted by the European Commission to govern the amount of capital insurers must hold against unforeseen events. ⁷³

Although these initiatives address a variety of substantive ills, they share certain important governance characteristics. Congress sets forth broad statutory aims and frameworks, but it delegates to administrative agencies the task of filling in the substantive detail. These regimes similarly articulate general goals yet largely delegate to regulated firms the decisions about specifics: everything from the meaning of the public aim in a particular context (e.g., identifying and mitigating a variety of risks, preventing financial fraud or misrepresentation, protecting sensitive information) to the means for achieving it. ⁷⁴ Certainly, some regulatory delegations (as with some statutory delegations) offer more precision than others, specifically requiring, for example, that regulated firms consider particular categories or types of risk. “Yet they make few ex ante decisions about substantive detail, leaving such decisions—at least in the first instance—to the regulated firm’s judgment.” ⁷⁵ To this extent, private firms are made partners in regulation,

⁷⁰ 17 C.F.R. § 240.15c3-4(a) (2009).
⁷¹ See supra note 26 and accompanying text.
⁷² See, e.g., STANDARD & POOR’S, REQUEST FOR COMMENT: ENTERPRISE RISK MANAGEMENT ANALYSIS FOR CREDIT RATINGS OF NONFINANCIAL COMPANIES (2007) (inviting industry comment on Standard & Poor’s proposal to include risk-management analysis in the credit-rating process).
⁷⁴ Bamberger, supra note 13, at 392. For several examples of these sorts of regulation delegations to the regulated private party itself, see Coglianese & Lazer, supra note 14, at 696–700.
⁷⁵ Bamberger, supra note 13, at 392; see also, e.g., Proxy Voting by Investment Advisers, 68 Fed. Reg. 6585, 6587 (Feb. 7, 2003) (codified at 17 C.F.R. pt. 275) (“We did not propose, and are not adopting, specific policies or procedures for advisers. Nor are we . . . providing a list of
implicitly and explicitly enlisted to fill out the substance of public legal norms. As I have argued elsewhere, such reliance on the judgment and decisions of actors in regulated firms is analogous to Congress's delegation to administrative agencies of the power to "fill in" regulatory details left open by statutory ambiguity. This parallel has powerful implications for administration.

Public law typically has little concern with the decisionmaking processes of private actors. It usually treats regulatory targets as unitary "black boxes," best motivated by regulatory specificity on the one hand, and external incentives in the form of outcome-based monitoring and sanctions on the other. And to the extent it does delve into private decisionmaking, it does so hesitantly, with a hands-off deference typified by corporate law's business judgment rule. These usual paradigms for thinking about regulatory compliance, however, provide a poor overlay for contexts in which "compliance" consists of good decisionmaking rather than fulfillment of particularized mandates.

By contrast, understanding regulated firms as partners in regulation suggests a different paradigm, one drawn from administrative law—the law that "regulates regulators." This paradigm "takes seriously the notions that policy solutions are complicated and varied, and that parties to whom discretion is given should employ their knowledge and judgment in the service of effective solutions." It thus emphasizes decisional accountability rather than rule following.

The accountability approach draws on detailed institutional accounts of the strengths and weaknesses of the participants and methods involved in making regulatory judgments. The approach relies on a variety of inputs and processes in structuring and overseeing the decisionmaking processes. Substantively, it aims to ensure that regulatory choices are made consonant approved procedures. Investment advisers registered with us are so varied that a 'one-size-fits-all' approach is unworkable. By not mandating specific policies and procedures, we leave advisers the flexibility to craft policies and procedures suitable to their businesses . . . ."

76. Bamberger, supra note 13, at 381.
77. See, e.g., Timothy F. Malloy, Regulating by Incentives: Myths, Models, and Micromarkets, 80 TEXAS L. REV. 531, 531–32 (2002) ("Environmental regulation is all about using incentives to control behavior. . . . Many regulators rely upon a 'black-box' model in developing and evaluating environmental regulatory incentives directed at businesses.").
78. See In re Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967–68 (Del. Ch. 1996) ("[T]he business judgment rule is process oriented and informed by a deep respect for all good faith board decisions.").
79. See Bamberger, supra note 13, at 396–99 (discussing the challenges posed by the delegation of regulatory discretion); see also Paul Seabright, Skill Versus Judgement and the Architecture of Organisations, 44 EUR. ECON. REV. 856, 857–59 (2000) (discussing the difficulty in codifying standards for, or even monitoring, the exercise of judgment).
81. Bamberger, supra note 13, at 400.
with public-law values such as rationality, reviewability, and effectiveness in achieving goals set by the democratically elected Congress. But it recognizes that measures intended to channel discretion to these ends “must be informed by an understanding of the challenges to good decision making particular to the context.”

Informed by this paradigm, the following parts engage in a granular analysis of one manner in which firms increasingly exercise the discretion left to them by the regulatory delegations—resort to technology systems—and discuss the implications for accountable governance.

III. The Turn to Technology, and Its Benefits

Across industry and context, firms increasingly exercise their regulatory discretion through the deployment of information-technology systems. Risk management in the modern firm—financial firms especially—must contend with increased transaction volumes, increased complexity in financial offerings, proliferating compliance and reporting requirements across business lines, and the massive accumulation of data that results. As a result, traditional reliance on manual controls and stovepiped compliance responses simply cannot keep pace with the increasing complexity of compliance burdens and evolving levels of risk. In light of the increasing sophistication of technology offerings and the geometric increase in computer processing power as compared to cost, a consensus has arisen among regulators, corporate risk managers, and risk-management specialists that—for reasons of both efficiency and effectiveness—the trend towards embedding risk management in technology systems is inevitable.

82. Id. at 381.
83. Id. at 407.
85. See, e.g., id. (“The increasing . . . complexity of financial products traded is putting pressure on existing risk . . . .”).
86. See, e.g., CHRIS MCCLEAN & MICHAEL RASMUSSEN, FORRESTER WAVE: ENTERPRISE GOVERNANCE, RISK, AND COMPLIANCE PLATFORMS, Q4 2007, at 2 (2007) (noting the burdens placed on businesses by market demand, in particular, regulatory compliance, globally distributed business requirements, and multiple regulatory environments).
87. Donald Langevoort’s 1985 exploration of the increasing role of information technology in financial investing flagged early on the implications for public policy. See Donald C. Langevoort, Information Technology and the Structure of Securities Regulation, 98 HARV. L. REV. 747, 750 (1985) (proposing a regulatory agenda at a time that questions of “regulatory policy posed by technological advancement” were widely before the SEC, “at least in primitive form”).
88. See, e.g., ERNST & YOUNG LLP, CORPORATE REGULATORY COMPLIANCE PRACTICES 29–30 (2005) (documenting the number of companies that use technology to track compliance and management, monitor compliance controls, and handle regulatory reporting).
A. Technology's Efficiencies

While difficult to measure precisely, the costs of compliance with management-based risk regulations are significant.\(^8\) More broadly, even before the recent economic downturn, the proliferation of risk-management mandates in highly regulated areas of the economy has resulted in significantly faster growth in compliance costs than in net income.\(^9\)

For a variety of reasons, automating compliance and risk-management processes provides marked efficiencies at a time when compliance budgets are increasingly constrained by the competition for resources among business functions.

First, the greatest source of increase in compliance spending has arisen from compensation of staff responsible for manual oversight of compliance controls.\(^9\) Where functions can be integrated through technology, controls can be automated at a single time rather than by individual event or transaction. Second, the development of technology systems has permitted firms to streamline enterprise-wide risk-management compliance. Each new legal mandate brings a new set of requirements regarding data collection, management and security, as well as reporting and auditing obligations.\(^9\) Organizations have traditionally addressed each compliance mandate discretely, assigning responsibility to either the affected business units or focused compliance offices. Developing scalable technology-based systems and controls can significantly reduce the overlap caused by these compliance "silos."\(^9\)

Finally, automation has permitted the alignment of the compliance function with business operations. Compliance has traditionally been

\(^8\) See PriceWaterhouseCoopers LLP, Intelligent Risk Management & Compliance Cost Reduction 3 (2008) ("The last decade has seen an unprecedented increase in risk management spend[ing]... The costs of the risk management and compliance functions themselves are only a fraction of the true cost of risk and compliance activities. The true cost of implementation of the compliance and risk activities in the front, middle, and back office processes is generally multiple times the cost of the risk management, audit and compliance departments themselves.").

\(^9\) See Deloitte Ctr. for Banking Solutions, Navigating the Compliance Labyrinth: The Challenge for Banks 3 (2008), available at http://www.securitization.net/pdf/Deloitte/Compliance_17Jan08.pdf ("Compliance costs grew significantly faster than net income for financial institutions in our survey. While compliance spending as a percentage of net income for the financial institutions surveyed was 2.83% in 2002, by 2006 it had grown to 3.69%."); see also PriceWaterhouseCoopers LLP, supra note 89, at 3 ("The functions that make up the risk management and compliance activities of firms have grown well beyond revenue and inflation rates...").

\(^9\) Deloitte Ctr. for Banking Solutions, supra note 90, at 3.

\(^9\) See Michael G. Silverman, Compliance Management for Public, Private, or Nonprofit Organizations 203 (2008) ("Each new law, regulation, or compliance mandate brings with it a new set of requirements in such areas as records management, data security, and privacy...").

\(^93\) See id. at 212 (discussing the advantages of a "holistic, multidimensional approach to technology utilization" in compliance frameworks).
managed separately from the risk-management function exercised by operational managers.\textsuperscript{94} Integrating compliance efforts with technology systems developed as part of overall enterprise-risk-and-governance functions further reduces redundancies while increasing the internal organizational influence claimed by compliance officers.

**B. Technology's Effectiveness**

At the same time as it can reduce costs, the tremendous computing power of information technology and process automation offers means for significant, qualitative improvement in the effectiveness of both compliance and underlying risk management.

Manual processes and controls are, themselves, a notorious source of operational risk. The functional discretion they permit to hundreds or thousands of individual decisionmakers at the very edges of large, modern corporations necessitates extensive training in complicated organizational business and compliance rules. This leaves openings for inconsistency, mistake, or outright fraud.\textsuperscript{95} Employee incentive systems complicate the balance of performance metrics with those measuring risk.\textsuperscript{96} Manual oversight and controls testing must typically be limited to spot-checks because of workload constraints.\textsuperscript{97} And systemic analysis of the flood of information that results, especially in data-intensive industries, is often impossible.\textsuperscript{98} The variety of data management and analysis tools available through modern information-technology systems offers firms a means to address each of these shortcomings.

\textsuperscript{94} See, e.g., DELOITTE CTR. FOR BANKING SOLUTIONS, supra note 90, at 15 (discussing the belief of some executives that integrating separately conducted compliance and risk-management activities would reduce the costs of duplication and provide a better perspective on the operations of the enterprise).

\textsuperscript{95} See Suzanne Dickson, Compliance Automation: Software Tools Can Give Auditors More Insight into the Controls and Policies Their Organization Needs to Meet Regulatory Mandates, INTERNAL AUDITOR, Feb. 1, 2007, at 27, 27 (“With so many different regulations to consider across an entire enterprise, it is nearly impossible to correlate business requirements with regulations and policies without an automated tool set.”).


\textsuperscript{97} Some companies spend upwards of 90% of their monitoring budgets on manual oversight. See SILVERMAN, supra note 92, at 143 (citing a 2006 report by the Securities Industry and Financial Markets Association showing that compliance staff was by far the largest cost item of a compliance program). Furthermore, the quality of such manual controls tends to decrease as workload increases. See Anne M. Marchetti, Monitoring: The Behavioral Economics of Corporate Compliance with Law, 2002 COLUM. BUS. L. REV. 71, 93 (asserting that even professional auditors rely on simplifying cognitive heuristics that are less precise when they have oversized workloads).

1. The IT Toolbox.—The power of information-technology systems arises from their ability to manage, organize, and analyze massive amounts of data with uniformity and particularity and then to structure decision-making accordingly.

Most simply, computer systems permit the creation of a consistent identification scheme for digital information across all business units (categories ranging from social-security numbers to internal losses), the integration of coded data from the breadth of firm operations, the identification of each system user, and a record of the source and treatment of data over its lifetime. Such systemic coding permits the organization, analysis, and mining of such data in ways that can radically alter decisionmaking premises.

Second, software systems can be developed to automate operational decisions based on this data according to rules adopted to manage risk—rules that reflect both business policies and formal regulations. Software code is rule based in nature, and automated decisionmaking software tends to be formed primarily of declarative logical statements that can be combined into decision-tree-like branches. Yet, while simple rules might be formed (such as “Do not let X user access both Y and Z type of personally-identifiable information,” or “Do not offer a mortgage requiring a monthly payment over $A to an applicant making less than $3A”), code’s rule-based nature does not imply any kind of simplicity inherent to software systems. Indeed, the ability to integrate an almost unlimited number of variables, informed by both risk and performance concerns, into automated decision rules means that “[s]oftware can successfully apply rules whose complexity would make them collapse under their own weight if humans were forced to apply them.”

Finally, technology systems permit more complex analysis of information through the use of data mining and analytics. Mining generally involves the identification of trends and patterns in large data sets, while analytics commonly refers to the “extensive use of data, statistical and quantitative analysis, explanatory and predictive models, and fact-based management to drive decisions and actions.”

---


100. See generally id. (discussing the ways in which business decisionmaking processes are streamlined by management information systems).

101. See JAMES TAYLOR, SMART (ENOUGH) SYSTEMS: HOW TO DELIVER COMPETITIVE ADVANTAGE BY AUTOMATING HIDDEN DECISIONS 150 (2007) (explaining that decision trees effectively describe systems where multiple rules share initial conditions and where each rule produces only a single outcome).


103. TAYLOR, supra note 101, at 112.

Technologies of Compliance

commonly employ regression, case-based reasoning, link analysis, clustering, and genetic algorithms—provide insight into the probability of specific outcomes, usually by analyzing large sets of historic data. Such quantitative analysis provides the cornerstone of modern risk analysis.\textsuperscript{105}

When combined with rule-based code, analytic modeling yields powerful capabilities. Executable software, drawing on both rules and analytics, can “sense online data or conditions, apply analytical algorithms or codified knowledge . . . and make decisions—all with minimal human intervention.”\textsuperscript{106} Such “business intelligence” software can thus “analyze, forecast, predict, [and] optimize” as well as “collect[], manag[e], and report[] decision-oriented data.”\textsuperscript{107} These functions are essential for compliance, not only with procedural risk-management mandates but also with regulatory reporting requirements. As one commentator describes, Sarbanes–Oxley requires that users of corporate data “demonstrate that their decisions are based on trustworthy, meaningful, authoritative, and accurate data.”\textsuperscript{108}

2. \textit{GRC Systems}.—The combination of these three functionalities provides the foundation for a variety of technology products and systems geared towards corporate risk management. Such systems are, in rare instances, developed within the user institution but, for the most part, are sold and developed by a variety of private third-party vendors.\textsuperscript{109}

The products and systems available in the market differ in scope and offerings. Industry leaders such as Axentis Inc.; BWise, Inc.; IBM; OpenPages, Inc.; Oracle Corporation; SAP AG; and Thomson Reuters Corporation provide comprehensive compliance- and risk-management platforms with packages geared towards a variety of the more common regulatory regimes such as Basel II, SOX, and various privacy and fraud laws.\textsuperscript{110} SAP’s compliance solutions even include offerings targeted to compliance

\textsuperscript{105} ANTHONY TARANTINO, GOVERNANCE, RISK, AND COMPLIANCE HANDBOOK: TECHNOLOGY, FINANCE, ENVIRONMENTAL, AND INTERNATIONAL GUIDANCE BEST PRACTICES 217 (2008) (describing how these risk analysis techniques permit discovery of phenomena that are “likely to be genuine” rather than “merely chance occurrences”).

\textsuperscript{106} DAVENPORT & HARRIS, supra note 104, at 150.

\textsuperscript{107} Id. at 155.

\textsuperscript{108} Id. at 156. The Act also requires testimony that “the data provides a clear picture of the business, major trends, risks, and opportunities.” Id.; see also TAYLOR, supra note 101, at 31 (discussing the role of systems in satisfying requirements that regulated parties not only comply with regulations but also demonstrate that compliance).

\textsuperscript{109} See Shazia Sadiq et al., Modeling Control Objectives for Business Process Compliance, in BUSINESS PROCESS MANAGEMENT 149, 149–50 (Gustavo Alonso et al. eds., 2007) (listing major compliance-system vendors).

\textsuperscript{110} See Fred Caldwell et al., Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms (Gartner RAS Core Research Note G00169604, Aug. 12, 2009), available at http://mediaproducts.gartner.com/reprints/oracle/article92/article92.html (identifying primary third-party vendors of GRC products and evaluating them on “completeness of vision” and “ability to execute” criteria); McCLEAN & RASMUSSEN, supra note 86, at 16–22 (making a similar evaluation of vendors based on “strategy,” “current offering,” and “market presence” criteria).
with the Clean Air Act and the Bioterrorism Act. Other companies offer targeted add-on or stand-alone products geared to more specific requirements, such as the mark-to-market reporting requirements in Financial Accounting Standards Board (FASB) Rule 157, or the European Union’s REACH regulations governing reporting substance volumes and other data by the chemical industry.

As a whole, however, the market is converging on a unified model of GRC software intended to harmonize and unify risk and compliance activities across all business lines. Such platforms promise a holistic view of risk across a firm by establishing a common methodology for assessing risk data arising from the range of risk sources, implementing procedures that mitigate risk, and providing a means for internal and external oversight. Thus, GRC technology focuses generally on four basic operations that, although they overlap to some degree, might be divided roughly as follows: (1) risk identification and measurement; (2) controls that force compliance with company-wide policies, including those informed by legal regulations; (3) monitoring of the risk-management system itself; and (4) compliance with reporting requirements.

a. Identification and Measurement of Key Risks.—The foundation of GRC systems is their ability to track and measure important sources of risk. Once key risk indicators have been identified and metrics for assessment developed, they can be systemically monitored, and processes for their mitigation can be implemented.

Some of the risks tracked by standard GRC systems are universal, such as compromised or inaccurate data, the improper allocation of decisionmaker...
Technologies of Compliance

...authority in ways that permit fraud or obscure oversight, or, on the other extreme, the risk arising from a lack of coordination between multiple actors participating in a single decision. Others are sector- or activity-specific, such as credit risk inherent in banking activity, or market or liquidity risk arising from particular financial-investment choices.

The process of identifying key risks in a technology system permits users to integrate more traditional, qualitative assessments of risk types, such as the comparative importance and severity of different types of risk to a particular business. More distinctively, however, the analytic capabilities of technology systems further permit a means for quantifying such risks by applying computational modeling and algorithms to data drawn from both within a corporation and external information sources. Both large and specialized vendors offer comprehensive analytics, for example, that model risk for the purposes of Basel II capital-adequacy requirements, banking soundness and safety compliance, and other regulatory regimes. Oracle’s Reveleus Basel II solution, for example, promises “a fully transparent ‘ready to go’ set of advanced analytical applications that combine pre-built data structures, pre-packaged computational engines, pre-designed information delivery templates, and a unifying reference language.”

The technology, with which Standard & Poor’s has partnered to provide its RiskComply product for investment managers, offers a “stochastic multi-factor risk model and advanced component Monte Carlo methods to calculate the risk” of holdings and compares it to limits specified by regulators in the client’s local territory, such as the European Union’s UCITS III directive governing hedge-fund management. Innovations Software Technology GmbH, which just entered into an agreement to provide risk-management analysis to...

---


Fannie Mae offers fifteen computational models for credit-risk assessment.

In this manner, the process of risk measurement can be automated. Key indicators are quantified; their trends are continually tracked; and their metrics are aggregated and compared.

b. "Forcing" Compliance Through Controls.—Once risks have been identified and means for measuring them developed, GRC systems establish decision controls that automate business "rules" intended to mitigate those risks consistent with both operational and regulatory requirements. The foundation for these business rules are frequently out-of-the-box policies developed by system vendors based on their understandings of industry best practices and compliance requirements. Sophisticated users, moreover, can work with vendors to tailor rules to their firm or to geographic variation in regulatory requirements, a process that may become easier as software developers design programs that automate tracking of which regulations apply to any particular transaction.

Automated controls employ a variety of mechanisms limiting what users can do, thus reducing their decisionmaking discretion. Access controls enforce rules prohibiting the linking of different types of information that must remain independent and ensure that only those users who should be able to see certain data can do so, automating compliance with data-privacy and security mandates. They are also central to ensuring the integrity of financial information at the heart of Sarbanes-Oxley compliance. Segregation-of-duties controls automate rules ensuring oversight over procurement and other operational decisions, limiting employee fraud or mismanagement.

120. See Innovations Software Tech., Customers, http://www.innovations-software.com/customers.html (listing Fannie Mae as one of the company's customers).


122. See Archer Tech., GRC Solutions for Retail, http://www.archer.com/solutions/industry/retail.html (providing an example of an industry for which an out-of-the-box GRC solution was developed).

123. See, e.g., Compliance 360, Solutions: Compliance Management, http://www.compliance360.com/solutions_compliance_management.asp (providing an example of a compliance management solution that features "an easily accessible, real-time view of all activities and documentation directly linked to specific laws, regulations and other requirements," as well as automated alerts of changes to those laws and regulations).

124. See, e.g., Oracle Corp., GRC Technology Controls, http://www.oracle.com/solutions/corporate_governance/grc-technology-controls.html (advertising a GRC system that employs user-access control and segregation of duties to comply with regulatory mandates for access to sensitive information).

functions can permit the uploading of information without the type of human intermediation that can permit fraud or inadvertent entry error. Automated permissions and record-keeping systems, moreover, are critical to informational integrity, as they can identify the source of each piece of information entered into a system as well as every employee who ever accessed it, and they can limit the changes that can be made.

The computing power of GRC systems, moreover, brings automation one step beyond merely directing what individual employees can access or do and establishes rule systems for governing complex business-decision processes themselves. Loan originations, for example, have been largely automated based on the characteristics of the borrower and the level of risk already held by a bank. Furthermore, technology systems can develop rule-based systems that “act” upon quantitative assessments of risk, governing business-wide decisions as to the types of assets that should be sold—or levels of capital increased—to satisfy both qualitative assessments of a firm’s risk tolerance and the requirements of governing law.

\[c. \text{Monitoring Risk Management.} - \text{The capacity to quantify risk, and then use those measures to automate business rules, underlies the most transformative aspect of GRC technology systems: the profound ways in which it facilitates auditing of risk management and the monitoring of risk as it develops.}\]

Oversight of the risk-management function is critical to legal compliance. Regulations routinely require the regular testing and monitoring of control effectiveness. The COSO framework, the privately developed risk-management best-practices framework that has largely guided firms’ compliance approach to Sarbanes-Oxley and other regulations mandating internal controls, emphasizes the role of corporate management in monitor-

---

126. See McCLEAN & RASMUSSEN, supra note 86, at 3 (asserting that GRC platforms will evolve and begin to incorporate business-logic and business-rules engines); see also, e.g., Fair Isaac Corp., FICO Blaze Advisor Business Rules Management, http://www.fico.com/en/Products/DMTools/Pages/FICO-Blaze-Advisor-System.aspx (providing an example of a Business Rules Management System (BRMS) software product that automates business decisionmaking in accordance with preestablished rules).


129. E.g., 16 C.F.R. § 314.4 (2009) ("In order to develop, implement, and maintain your information security program you shall: . . . (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems, and procedures.").
The U.S. Sentencing Guidelines, which have shaped the understanding of regulatory requirements across contexts, require that, to be considered effective, a compliance program must be administered and overseen by high-level personnel within the organization and must include appropriate monitoring and auditing systems. And the case law governing the fiduciary duty of corporate boards articulates a director's "duty to attempt in good faith" to assure that an adequate corporate information and reporting system exists, a task integral to the requirement that the director be "reasonably informed" about a corporation's operations.

GRC systems offer the means for automating this audit and oversight function, principally by establishing baseline measurements for all major operating systems, continually monitoring key risk indicators, and then automatically identifying "exceptions" to baselines, as well as risk trends.

Such automated detection features offer significant strengths over traditional forms of audit. While manual control testing typically relies on spot-checking sample transactions or data, automated, rule-based systems can test or audit every relevant transaction or database and do it more independently and accurately. Such uniformity in testing and reporting further permits the use of the data for benchmarking and monitoring of changes in key risks. Automated systems can thus comprehensively identify incidents inconsistent with governing rules and policies, as well as patterns that might reveal changes in risk exposure. This permits oversight of both internal controls themselves and the risk they are intended to manage in three important ways.

i. Automating the Audit Function.—First, and perhaps most basically, GRC systems offer a comprehensive audit function for assessing how well a company's compliance processes are performing. This is done

130. See COSO, supra note 49, at 3-4 (indicating that the COSO framework includes components of risk-response and risk-management-system monitoring); id. at 6 (indicating that several levels of management play key roles within the COSO framework).


132. See In re Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996) (holding that corporate boards have an "obligation to be reasonably informed"); id. ("[A] director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists ....").

133. See Scott Leibs, One for Three: Should Governance, Risk Management, and Compliance Be Tackled as One Problem, or Is This a Classic Case of Scope Creep?, CFO MAGAZINE, Sept. 1, 2007, available at http://www.cfo.com/article.cfm/9689509/1/e_29844097/=archives (describing that GRC software "[a]t its core...remains a tracking system, capturing data on various compliance requirements as they affect a specific company and chronicling how the company does (or does not) satisfy those requirements"); see also Brian Klemm, The Genius of Compliance Technology, CORP. COMPLIANCE INSIGHTS, Feb. 3, 2009, http://www.corporatecomplianceinsights.com/2009/genius-of-compliance-technology ("In order to effectively prevent problems and manage risks, compliance professionals are implementing controls and measuring and monitoring them with metrics to evaluate how well such controls are performing.").
Technologies of Compliance

principally by automated, periodic testing of the controls themselves, as well as by continuous monitoring to "detect, after the fact, system transactions, setup, or data changes that contravene corporate policy." Vendors offer different manifestations of what they often refer to as an executive dashboard, which provides responsible managers with a visual computer-screen overview of tasks or relevant information pertaining to the performance of a particular control. Tied to these dashboards are incident- or exception-monitoring tools that automatically document and feed alerts to key staff members when certain compliance or policy rules are broken, consistent with legal regimes such as Basel II that require registration of incidents, near-incidents, and unforeseen surprises.

These systems further assess the effectiveness of real-time compliance controls by monitoring completed transactions and decisions in light of predictive analytics developed to identify risky events. Such events may include unusual transactions that might indicate money laundering, insider trading, or transactions that, while not out of the ordinary in and of themselves, are exceptional in comparison to other transactions made during a similar time period.

This functionality was critical in the discovery in 2005 of massive fraud at Refco, Inc., a commodities and futures trading company. The firm’s CEO had been hiding debts by borrowing money from a hedge fund before each quarterly report and returning it afterwards. While this behavior continued for a number of years, audit mechanisms, put into place in advance of the firm’s planned IPO in 2005, flagged those deals as exceptional because the interest rates charged by the hedge fund were markedly higher than the pattern of interest rates paid on other loans during similar periods. The resulting investigation into the loans led to the discovery of the underlying debts and the firm’s bankruptcy—the fourth largest in U.S. history at the

134. TARANTINO, supra note 105, at 309.
138. Id.
139. Id.
Automated, continuous monitoring tools permit risk managers to identify control failures earlier and flag risks that existing controls may simply have missed by design, and then, where possible, to alter the automated business rules and policies accordingly.

ii. Centralizing Risk Oversight.—Second, GRC systems inject transparency into an organization's entire risk landscape by permitting centralized managers to view, in an updated manner, risk measures from the breadth of risks identified across the firm. Continual monitoring of key risk indicators permits tracking of the trends of each type, while the integration of risk measures within a single platform increasingly permits their aggregation and comparison.

In this fashion, technology provides a means for ameliorating traditional problems of information asymmetry that result from specialization and division of labor—critical structural elements of efficient firm organization. For a variety of structural and cognitive reasons, formal lines of organizational communication are often poor conduits for ensuring that information about risk, in particular, gets from those who possess it to those who might act on it. Localized sensitivity towards risk and change amongst those lower down in the corporate structure is often difficult to codify formally. Risk information may also be understood, in light of a firm’s culture or incentive structure, as a sort of proprietary input to decisions located within a particularized business unit.

141. See Klemm, supra note 133 (“Technology can enhance visibility into an organization’s risk landscape—including strategic, operational, reporting, compliance, market, credit and technology related risks . . . ”).
142. See RICHARD H. HALL, ORGANIZATIONS: STRUCTURES, PROCESSES, AND OUTCOMES 169 (8th ed. 2002) (“If the total rationale for all actions were known to all members, the potential for chaos would be high, since communication overload would quickly occur.”).
143. See John C. Coffee, Jr., Beyond the Shut-Eyed Sentry: Toward a Theoretical View of Corporate Misconduct and an Effective Legal Response, 63 VA. L. REV. 1099, 1137–39 (1977) (discussing the “problems associated with the upward transmission of adverse information within the corporate hierarchy”).
145. See Coffee, supra note 143, at 1135–36 (explaining the theory of “subgoal pursuit,” which is that “given an opportunity to exercise discretion, managers at lower levels within a firm will tend to act not to maximize the firm’s welfare, but rather the interests and autonomy of their own unit or division”).
Even in a firm with effective communication systems, summaries and overviews provided to managers can displace specific detail as not all information can be included in upward communications or reports. Predictable cognitive and systemic processes, moreover, can bias this editing process as, for a variety of reasons other than guile, people are less likely to pass information up if it will be harmful to themselves or their peers. Specifically, pursuant to the theory of cognitive dissonance, "recipients of information unconsciously focus on and relay only the information that reinforces their preexisting attitudes while filtering out conflicting information." This effect is exacerbated in cases in which upward communications contain early tentative warnings about risk shifts; in such cases, a busy upper-level manager, in winnowing down information for attention and further transmission, may focus on what are perceived as more immediate problems, leaving others for resolution in the business unit itself.

By automatically unearthing and aggregating data across business roles and functions, on the other hand, technology systems can elevate timely and accurate information about loss incidents, gains, market shifts, and other data implicating risk to each actor responsible for thinking about risk—risk managers, risk owners in lines of business, executive management, and even the board audit committee. The dashboards of leading GRC systems feature home pages that provide executives with a bird's-eye view of different types of risk. They document risk levels and compliance activities, and permit immediate access to reports with metrics and charts indicating the status of these activities. In industries like investment management, banking, and insurance, in which taking on and balancing different types of risk inheres in the strategic business model, the increasing capacity to centralize access and oversight of the risk exposure of different and geographically dispersed business units has become an especially critical systems function.

iii. Real-Time Decision Support for Risk Mitigation.—Finally, as computing capacity expands and monitoring begins to approach real

146. Id. at 1139.
147. See Donald C. Langevoort, Organized Illusions: A Behavioral Theory of Why Corporations Mislead Stock Market Investors (And Cause Other Social Harms), 146 U. PA. L. REV. 101, 135–39 (1997) (noting the common norm in business to only communicate information upward that is significant and unusual as one reason why cognitive conservatism and decision simplification limit the communication of risk).
148. See supra notes 135–36 and accompanying text.
149. See IBM Corp., supra note 135 ("Role based dashboards provide visual views of risk and control environment status."); SAP AG, supra note 125 ("You can gain continuous visibility across compliance initiatives via accountability and standardization of processes, together with comprehensive reports and dashboards to monitor effectiveness across systems.").
technology systems' ability to aggregate data, apply rules that embed baselines and risk-measurement analytics, identify exceptions, and distribute information widely increasingly provides transformative decision-support tools and enables businesses to "manage by exception." The faster GRC systems can enable automatic input from various data sources to track key risk indicators, the more effectively they can compare predicted baselines and thresholds to actual performance and identify "exceptions" so that timely action can be taken to minimize losses and avoid exposure.

The promise of these nascent tools for identifying early warnings of change within an organization's risk profile is extremely important not only for business reasons but also for public policy. Specifically, they offer an important means for overcoming predictable decision pathologies, which research on decisionmaking in organizations demonstrates can mask the very type of risks and dangers targeted by regulation.

Such decision pathologies arise from the ways in which organizational decisionmaking is shaped by the realities of individual cognitive capacity. As the literature on cognition has explored, the human mind faces biological constraints on its perceptual and computational capacity—human decision-makers can never hope to process all available information about all possible choices or consider the implications of every decision. We adapt to these shortcomings by developing cognitive shortcuts that generally make it easier to make sense of new situations, even in the absence of complete information. For instance, biases or heuristics allow us to take cues from familiar aspects of a situation, to assess unfamiliar settings, and to trigger rules of decision.

Organizations, in turn, provide the particular settings that shape those knowledge structures: the rules and procedures for making sense of situations and identifying the appropriate response quickly. Such structures provide

---

151. See generally Steve Hamm, IBM Roars into Business Consulting, BUS. Wk., Apr. 15, 2009, at 10, 10 (discussing a test system developed by IBM and run on one of its Blue Gene supercomputers permitting financial-services company TD Securities Inc. to analyze options-trading data in real time and make adjustments in microseconds).

152. See PETER G. NORTHOUSE, LEADERSHIP: THEORY AND PRACTICE 185 (4th ed. 2006) (defining management by exception as "leadership that involves corrective criticism, negative feedback, and negative reinforcement").


154. See Bamberger, supra note 13, at 383–84 (observing that private firms with regulatory discretion suffer from accountability problems and irrational decisionmaking).


156. See HERBERT A. SIMON, ADMINISTRATIVE BEHAVIOR, at xxix (3d ed. 1976) (remarking that humans consider only a few possible courses of action and choose to settle for a solution that is adequate rather than "maximizing").
shortcuts that enable individuals within an organization to identify the type of challenge they face efficiently, to focus their attention on the kind of information needed for that sort of situation, and to invoke an applicable rule of behavior swiftly. These structures include formal top-down rules, embodied in standard operating procedures, handbooks, and organization charts.157 They also include bottom-up rules developed on the ground through the evolution of informal routines and rules of thumb.158 By storing organizational knowledge in this way, routines shape the lenses through which events are perceived, "allow[ing] reuse of solutions to problems,"159 which, in turn, allows organizations to find "good, even optimal, rules for many choices they are likely to face."160

Yet this organizational source of strength can also create predictable decisionmaking pathologies by rendering decision makers insensitive to change, the source of risk. These knowledge structures accentuate familiarity—what is cognitively available161—and deemphasize difference, masking red flags that might indicate troubling elements of new situations. Once this occurs, the problem is exacerbated by a number of other phenomena. "Commitment" or "confirmation" effects prompt decisionmakers to seek out and emphasize information of the type that reinforces the familiarity of new, and potentially problematic, situations, biasing subsequent analysis toward data that confirms the initial interpretation.163 In

157. See RICHARD M. CYERT & JAMES G. MARCH, A BEHAVIORAL THEORY OF THE FIRM 113 (1963) ("These rules are the focus for control within the firm; they are the result of a long-run adaptive process by which the firm learns; they are the short-run focus for decision making within the organization.").

158. See id. (arguing that organizations use "rules of thumb" to make and implement choices and that these procedures dominate the decisions made in the short run).


160. JAMES G. MARCH, EXPLORATIONS IN ORGANIZATIONS 67 (2008).

161. See generally Amos Tversky & Daniel Kahneman, Judgment Under Uncertainty: Heuristics and Biases, in JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES 3, 11–14 (Daniel Kahneman et al. eds., 1982) (discussing the tendency to assess the "frequency of a class or the probability of the event by the ease with which instances or occurrences can be brought to mind").

162. See, e.g., DAN MAYER, ESSENTIAL EVIDENCE-BASED MEDICINE 193–94 (2004) (describing doctors' tendency, due to the availability heuristic, to look for similar causes of recently treated symptoms, thereby overlooking other causes).

163. For discussion of "commitment" or "confirmation" biases, see generally Jürgen Beckmann & Julius Kuhl, Altering Information to Gain Action Control: Functional Aspects of Human Information Processing in Decision Making, 18 J. RES. PERSONALITY 224 (1984), discussing findings that individuals make use of selective changes in information processing depending on personal goals; Hillel J. Einhorn & Robin M. Hogarth, Confidence in Judgment: Persistence of the Illusion of Validity, 85 PSYCHOL. REV. 395 (1978), explaining the persistence of individuals' overconfidence in judgment through learning models; Jonathan St. B.T. Evans, Beliefs and Expectations as Causes of Judgmental Bias, in JUDGMENTAL FORECASTING 31, 33 (George Wright & Peter Ayton eds., 1987), describing confirmation bias as the theory "that people's thinking is channel[ed] and biased by prior beliefs and expectations which inhibit logical reasoning"; and Barry M. Staw, The Escalation of Commitment to a Course of Action, 6 ACAD. MGMT. REV. 577 (1981), exploring the observed tendency to escalate commitment in the face of losses. For
this way, individuals unconsciously “make the problematic nonproblematic” by shielding themselves from information that may disprove the applicability of preexisting categories to new situations, even if the result is to ignore red flags and respond inappropriately.

Donald Langevoort has explored the ways in which these problems are exacerbated in the organizational culture of financial institutions. Such institutions’ strong incentive and reward structures can, in particular, enhance a “self-serving bias”: a cognitive phenomenon by which the mind naturally interprets ambiguous information in a manner favorable to the perceiver. This permits decisionmakers the self-deception that the group interest is “in full consistency with their personal goals.” The optimistic “can-do” outlook developed in financial-trading culture, moreover, exacerbates an individual’s “tendency to underestimate or rationalize risk” by shaping the interpretation of early, and still ambiguous, information. Once managers have publicly committed to expressions of optimism, they are to some extent cognitively locked in to the approach. Their optimistic perceptions are entrenched by their commitment, and they interpret and winnow new information consistent with their self-interest. Accordingly, fewer danger signs will raise red flags. These effects, Langevoort suggests, are important in answering the question of why public corporations mislead stock-market investors given that this behavior “simply delays the appreciation of the truth rather than avoids it indefinitely” and is ultimately uncovered.

The literature on organizational learning, however, suggests the promise of GRC technology systems in overcoming obstacles to the type of risk identification and management important to regulators. Specifically, it points to the potential of these systems’ capacity to establish rule-based benchmarks and to automate real-time collection of data indicating “exceptions” and

---


165. See Langevoort, *supra* note 147, at 107 (discussing the effect of biased information processing on firm-management behavior).


167. Langevoort, *supra* note 147, at 144.

168. Id. at 141.

169. Id. at 106.
trends deviating from such baselines. That body of research identifies effective benchmarking measures as particularly effective tools in prompting decisionmakers to take account of information that their knowledge structures might otherwise filter out.

Indeed, benchmarking has been identified as a particularly powerful means of prompting decisionmakers to replace routinized identification and interpretation of information with what has been called “mindful scanning” of the informational environment. It prompts decisionmakers to focus attention on small changes “on the fringes of current operations,” which dominant knowledge structures might mask as anomalous, yet may be the best indicators of risk.

This capacity is further suggested by the case, discussed at the outset, of Goldman Sachs, whose success in avoiding the fate of numerous competitors has been attributed to its risk-management system. That system’s predictive risk-analytic methods and tests of risk exposure, such as scenario analysis and stress testing, produced the early reports that flagged a trend of small losses in the firm’s mortgage business—losses that, viewed individually, might not have seemed out of the ordinary. The ability to recognize and respond to such changes on the margins proved central to Goldman’s viability. The firm even claims that if insurer AIG had been allowed to fail in September 2008, Goldman would not have been materially hurt, despite the fact that it held $13.98 billion in CDOs written by AIG.

d. Compliance with Reporting Requirements.—Finally, and perhaps most straightforwardly, technology systems have become necessary for compliance with legal reporting and disclosure requirements. While risk-
management mandates leave great discretion as to the development of the systems required to assess and manage risk, they provide far greater specificity as to deliverables that must be filed with administrative agencies and disclosed to the public.\textsuperscript{179} Any single firm can be subject to a number of overlapping yet distinct reporting requirements. These range from reports that must be filed at regular intervals, such as quarterly financial reports,\textsuperscript{180} to those that are event triggered, such as data regarding banking losses\textsuperscript{181} and the Suspicious Activity Reports required by the Bank Security Act and the USA PATRIOT Act within thirty days of discovery of transactions flagged under metrics intended to track internal abuse or money laundering.\textsuperscript{182}

For large firms especially, and for an increasing number of small and medium entities, such requirements necessitate the ability to store and aggregate data across business entities, relationships, risk categories, event types, and time periods that only sophisticated technology systems provide. More specifically, they require the technological ability to reorganize and offer different ways of analyzing and presenting different slices of the firms’ data so that it conforms with different regulator preferences, including financial accounting regimes, incident-report requirements, and electronic-filing formats.

IV. Technology Pitfalls and the Challenge for Governance

The identity between risk management and technology systems, then, has become increasingly exact. Especially for large corporations whose behavior most implicates public policy regarding market stability, the demands of data collection, manipulation, and analysis, embodied in the risk-management frameworks endorsed by regulators, simply cannot be met by manual processes or even the stand-alone spreadsheet offerings of earlier digital generations. Thus, if management-based governance regimes delegate to regulated firms significant capacity to write the meaning of the law by means of its implementation, the inevitable turn to technology in risk management takes this law-elaboration function one step further.

\textsuperscript{179} Information disclosure is a central feature of many regulatory regimes, notably those governing financial and environmental matters, and is geared toward fostering market or political accountability through the dissemination of accurate information that would otherwise remain hidden within firms. \textit{See generally} Cass R. Sunstein, \textit{Informational Regulation and Informational Standing: Akins and Beyond}, 147 U. PA. L. REV. 613, 618–25 (1999) (discussing those compelled disclosures that are meant to affect market responses and those meant to affect political responses).


\textsuperscript{181} \textit{See} 17 C.F.R. § 240.13a-11 (2009) (requiring registrants to file a current report on Form 8-K within the time period specified on that form); SEC, FORM 8-K §§ 1–6, \textit{available at} http://www.sec.gov/about/forms/form8-k.pdf (specifying triggering events—bankruptcy, disposition of a significant amount of assets, and material impairments—that require registrants, in most cases, to file Form 8-K within four business days of the events).

\textsuperscript{182} \textit{See} 31 C.F.R. § 103.18 (2009) (detailing the characteristics of transactions that would require an entity to file a Suspicious Activity Report).
As scholars of information technology have described, such technology functions, itself, as a newly salient regulator;\textsuperscript{183} its software code functions as law.\textsuperscript{184} Indeed, risk-management systems derive their strength from code’s rule-based ability to govern behavior, predetermine decision outcomes, and “specify completely the results of cases in advance without leaving space for situation-specific discretion.”\textsuperscript{185}

If firms exercise their regulatory discretion to meet public mandates through the bottom-up adoption of code, the question arises how, and to what extent, this “West Coast Code”—private implementation through the software emblematic of Silicon Valley—aligns with “East Coast Code”—the expectations of formal law emanating from Washington, D.C.\textsuperscript{186} Does it effectively promote the substantive concerns of governing legislation? Does it appropriately reflect the strengths of regulated parties whose judgment and informational advantage management-based regulation (new governance regimes) seeks to enlist? Do the ways risk-management regimes have developed sufficiently improve the responsiveness of corporate decision-making to the logic of law? In short, how does the technological instantiation of law-elaboration through implementation fare in light of the public-law norms of accountability, effectiveness, and legitimacy that traditionally govern the exercise of delegated discretion?

A. The Reticent Regulator

Spurring the development of state-of-the-art technology through regulatory mandates is not a new process. Indeed, legal scholars have long recognized the technology-forcing capacity of environmental regulation.\textsuperscript{187} By setting standards that regulated entities must achieve, public legal

\textsuperscript{183} See LESSIG, supra note 31, at 5 ("[Cyberspace] compels us to look beyond the traditional lawyer’s scope—beyond laws, regulations, and norms. It requires... the recognition of a newly salient regulator."); see also LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 5 (1999) (“Cybernetics had a vision of perfect regulation. Its very motivation was finding a better way to direct.”).

\textsuperscript{184} Reidenberg, supra note 31, at 554–55.

\textsuperscript{185} Grimmelmann, supra note 102, at 1732.

\textsuperscript{186} LESSIG, supra note 31, at 324.

mandates spur private technological innovation as regulatory targets develop state-of-the-art means for environmental compliance. Yet environmental regulation frequently involves the establishment of measurable outcomes, which permit the "re-entry" of the regulator into the process of gauging the effectiveness of technological compliance before risk has materialized into disaster. Management-based prescriptions regarding financial and operational risk, for the reasons explored in Part II, largely do not.

Moreover, although regulators formally recognize that the management-based mandates they promulgate regarding financial and operational risk necessitate a turn to technology, they have, with few exceptions, been reticent to participate in a robust way in shaping technological implementation.

To be sure, financial regulators have sometimes indicated their approval of particular approaches to risk management (such as the COSO framework) or to valuation metrics (such as the quantitative Value at Risk (VaR) models) relying on historical data that many GRC systems

188. See McGarity, supra note 187, at 945–47 (highlighting the EPA’s regulation of Mirex as an example of technology forcing succeeding in introducing new products to the market).

189. See Randle, supra note 187, at 1717–18 (commenting on the EPA’s standard-review powers under the Clean Air Act as a way to ensure that private companies continue to adopt control-technology improvements).

190. See, e.g., FED. RESERVE SYS., TRADING AND CAPITAL MARKETS ACTIVITIES MANUAL § 2040.1, at 1 (2003), available at http://www.federalreserve.gov/boarddocs/supmanual/trading/trading.pdf (“To manage their risk-management process in the current financial and technological environment, financial institutions are more readily prepared to incorporate the latest communications systems and database management techniques. In addition, new financial concepts are rapidly becoming standard practice in the industry, made possible by powerful computing tools and communications systems.”); FED. RESERVE SYS., DIV. OF BANKING SUPERVISION & REGULATION, LETTER SR 00-3, INFORMATION TECHNOLOGY EXAMINATION FREQUENCY 1 (2000), available at http://www.federalreserve.gov/boarddocs/srletters/2000/SR0003.htm (“Banking organizations increasingly rely on information technology to conduct their operations and manage risks.”); OFFICE OF THE COMPTROLLER OF THE CURRENCY, BULLETIN NO. 98-3, TECHNOLOGY RISK MANAGEMENT 4 (1998), available at http://www.ffcic.gov/ffcicinfobase/resources/info_ser/sec/occ-bu98-3_technology_risk_management.pdf (“Today, technology has moved ‘out front’ into virtually all aspects of banking. Technology is a key aspect of many bank business decisions and many new bank products are reliant on new technologies. Uses of technology are integral to bank operations and have been a primary force in creating new competitive opportunities for banks.”); FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK 1 (2004), available at http://www.ffcic.gov/ffcicinfobase/booklets/operations/operation.pdf (“As the complexity of technology has grown, the financial services industry has increased its reliance on vendors, partners, and other third parties for a variety of technology solutions and services. Institutions will frequently operate or manage various IT resources from these third-party locations.”); U.S. DEPT. OF TREASURY, OFFICE OF THRIFT SUPERVISION, EXAMINATION HANDBOOK § 341.1 (2008), available at http://files.ots.treas.gov/422120.pdf (“Even the most traditional, conservative associations have embraced technology.”).

191. These exceptions, such as certain activities of the Federal Trade Commission and the Food and Drug Administration, discussed in Part V as models for innovation, occur largely outside the financial-regulation context.

192. COSO, supra note 49.

193. See infra notes 265–88 and accompanying text.
incorporate. Individual financial-institution regulators have, moreover, periodically exercised their soapbox capacity to "jawbone" regulated parties with informal guidance regarding the use of technology. Former Federal Reserve Governor Susan Bies, before she resigned in 2007 in apparent frustration at the slow pace of regulatory progress, delivered a number of speeches suggesting the components of a best-practices risk-management system while also appreciating that technology and business processes can themselves be a "growing source of risk exposures" that can be mitigated by certain "processes to identify potential sources of risk early in the design and implementation process." SEC officials, moreover, have touted the best practices characterizing an "evergreen" compliance program—a "state of constant improvement to identify and address new issues and compliance risks, incorporate new forensic tests and new technology."

Yet these same regulators have largely refrained from more active involvement in shaping risk-management practices. Rather than embracing the new governance view of the government's role in steering, these regulators have focused more heavily on mapmaking—a "look no hands" approach that leaves directional choices to development from the bottom up.

As the following discussion explores, however, this hands-off approach ignores the ways in which reliance on technology systems can mask the very types of risk that should concern policy makers. In turn, it overlooks the challenge posed by compliance choices for effective regulation and legitimate public administration.

B. The Perils of Technology

The regulatory language of automated "controls" reveals, at a minimum, a core faith in organizational capacity for tight implementation of risk-management goals through automated systems. Indeed, as described in Part III, technology systems can reasonably be described—as they are by regulators, vendors, and users—as powerful managerial tools that can be tailored to organizational needs and universal compliance, that are flexible in responding to change, and that increase visibility and oversight of business processes.

---


197. Richards, supra note 20.

198. See Akira Tsuchiya, Toward Effective eGovernment Implementation: Examining Characteristics of U.S. Internet Users, GEO. PUB. POL'Y REV., Fall 2004, at 41, 43 (stating that
Research into information systems, however, suggests the incomplete nature of this instrumental account of technology. Just as divergent logic governs legal and management systems, obstructing the ability of one to fully control the other, technology is constituted by a third, independent language that poses problems of translation from legal mandates to technological idiom. Information technology is not value-neutral, but embodies bias inherent in both its social and organizational context and its form. It is not infinitely plastic, but, through its systematization, trends towards inflexibility. It is not merely a transparent tool of intentional organizational control, but in turn shapes organizational definitions, perceptions, and decision structures. In addition to controlling the primary risks it seeks to address, then, it can raise—and then mask—different sorts of risk in its implementation.

1. Problems of Translation.—While technology systems, particularly in their ability to monitor benchmarks and flag exceptions, offer great capacity for ameliorating decisionmaking biases arising from structures of efficient management, they create distortions of their own. In particular, the use of technology systems to hardwire compliance raises a number of fundamental issues regarding the translation of both legal mandates and business understandings of risk into computer code and actionable controls.

These translation distortions arise from the organizational and social context in which translation occurs; choices "embody biases that exist independently, and usually prior to the creation of the system." And they arise as well from the nature of the technology itself—"limitations of computer tools such as hardware, software, and peripherals; the process of ascribing social meaning to algorithms developed out of context; imperfec-
tions in pseudorandom number generation; and the attempt to make human constructs amenable to computers.\textsuperscript{203}

In the risk-management context, these distortions arise at various points in the translation process. First, risk managers face the challenge of double translation in trying to codify their understandings of risk into (1) actionable, rule-bound controls that (2) they, or their legal advisors, also believe satisfy regulatory mandates. These requirements are then provided to engineers for further translation into computer code.\textsuperscript{204}

This process leads to numerous winnowing effects as to the breadth and nature of risk identification. The necessity of developing business rules that can be integrated into digital logic establishes a bias towards the knowable and measurable—or at least towards those types of risks that risk culture believes can be known and measured\textsuperscript{205}—as well as towards existing types of metrics. As such, the process tends to exclude from automation those things that cannot be automated, such as the more subjective indicators of risk arising from individual judgment within the organization,\textsuperscript{206} and risk managers embrace prevailing disciplinary notions—spread through business schools, industry associations, and consulting firms—regarding what types of risk can be quantified and measured.

This bias is exacerbated by the attempt to integrate legal and management ideas regarding the types of controls that can manage risk. To begin with, business rules may be poor vehicles for capturing nuance in legal policy,\textsuperscript{207} especially in a context like risk management where regulators have eschewed rules for standards.\textsuperscript{208} Moreover, the focus on internal controls as

\begin{flushright}
\textsuperscript{203} See id. at 335 (listing sources of technical bias that exist in the design process).
\textsuperscript{204} See Danielle Keats Citron, \textit{Technological Due Process}, 85 WASH. U. L.R. 1249, 1261–62 (2008) (indicating that policy distortions can arise when code writers—who lack "policy knowledge" and may themselves be biased—translate policy from human language to computer code).
\textsuperscript{206} See Claudio Ciborra, \textit{Imbrication of Representations: Risk and Digital Technologies}, 43 J. MGMT. STUD. 1339, 1345–47 (2006) (concluding that managerial practice often diverges from system predictions due to the latter’s reliance upon “purely technical perspectives, such as that of the ‘unbiased’ decision maker”).
\textsuperscript{207} See Citron, \textit{supra} note 204, at 1261 (hypothesizing that because artificial languages employ a more limited vocabulary than human languages, they “are unable to capture the nuances of a particular policy”).
\textsuperscript{208} See Vincy Fon & Francisco Parisi, \textit{On the Optimal Specificity of Legal Rules}, 3 J. INSTITUTIONAL ECON. 147, 147 (presenting a model of optimal specificity of laws that predicts the use of standards instead of rules in areas undergoing rapid change).
\end{flushright}
a mechanism for legal compliance, however useful it may be, can further skew the viewpoint of risk assessment towards backwards-looking metrics, for "[c]ontrol actions are based on feedback from a disturbance that has occurred. Risk, by contrast, is about future disturbances . . . ." 209

These distortions, finally, are compounded when requirements reflecting salient sources of risk, approaches to risk measurement, and controls for risk mitigation are turned over to experts, both of the programmer and "quant" varieties, for translation into predictive algorithms and computer code. 210 These experts may know nothing of the management of risk within organizations or of the law. 211 Some are employees of separate IT divisions within firms; many are employees of third-party systems vendors. Wherever they work, their translation efforts are colored by their own disciplinary assumptions, the technical constraints of requirements engineering, and limits arising from the cost and capacity of state-of-the-art computing.

Specifically, programming requires actors to "quantify the qualitative, discretize the continuous, or formalize the nonformal." 212 In an absolutely rule-bound discipline, discrete values must fix flexible concepts such as materiality or adequacy. Financial-product risk that might conceivably be subject to a variety of valuation methodologies will be isolated in a single measure, however complicated its analytic for choosing between, or blending, different approaches. The choice between the many ways to resolve this ambiguity, in turn, is shaped by the institution or individual making the decision. That decisionmaker faces limits on its own cognitive frames, as well as social, political, economic, and legal motivations in reaching its choice. 213

The choice will also be shaped by practical constraints on computing capacity and system cost. The case of Goldman Sachs's ability to detect a downward trend in mortgage-backed assets, for example, underscores the benefit of developing a monitoring capacity that approaches real-time feedback as closely as possible. Yet real-time calculations require massive computing power; IBM's touted recent test system, permitting a small

209. Ciborra, supra note 206, at 1346.

210. See Taylor, supra note 101, at 31 ("If more of your decisions are embedded in your information systems, however, you risk pushing the enforcement of these rules onto programmers who don't understand them, not onto businesspeople who do.").

211. See Citron, supra note 204, at 1261 ("Information technology consultants cannot be expected to have specialized expertise in regulatory or public benefits programs."). The "experts" may not even possess uniform expertise of their own. As one commentator has noted, "To put it bluntly, you can't be a quant if you can't code . . . . To put it blunter, you would be hard-pressed to find a finance academic who can code . . . ." Pablo Triana, Lecturing Birds on Flying: Can Mathematical Theories Destroy the Financial Markets? 68 (2009).

212. Friedman & Nissenbaum, supra note 199, at 334.

213. See Jay P. Kesan & Rajiv C. Shah, Deconstructing Code, 6 Yale J.L. & Tech. 277, 283 (2004) ("[Science & Technology Studies] examines how technology is shaped by societal factors such as politics, institutions, economics, and social structures.").
Technologies of Compliance

financial-services company to analyze options-trading data in real time, is housed on one of the computing giant's Blue Gene supercomputers—computers developed to surpass all existing processing speeds.

Moreover, like any choice to govern by rule rather than by standard, the ultimate choice will inevitably result in inexactness; it will be, in different ways, both over- and under-inclusive. Thus, John Walsh of the Office of Compliance Inspections at the SEC, in one of the most insightful regulator statements regarding compliance technology, warned of the dangers raised by firms' 'increasing reliance on electronic exception reports as foundational elements in their supervisory and compliance systems.' He described this reliance as a positive development. Yet he also cautioned:

If you set their parameters too high, they could miss important red flags. For example, if you have an electronic report that monitors for investment time horizons, but you assume that only investors under age 50 have investment time horizons, you could miss a lot of red flags relating to the elderly. Also, an electronic report cannot find red flags in data it does not have. For example, if you rely on your clearing broker for mutual fund exception reports, but do most of your business with the fund companies by way of "check-and-app," those clearing broker reports will not do you much good.

The problem is that "theoretical considerations—fundamental issues emanating from the creation, use and application of laws—create disparities between the computational representation and the law as it operates in practice." Even a rule that appears perfectly drafted is "almost always an

---

214. See Hamm, supra note 151, at 10 ("IBM built a test system for financial-services company TD Securities that lets it analyze options trading data in real time and make adjustments in microseconds. The system, run by IBM on one of its Blue Gene supercomputers, improved the performance of the trading system by a factor of 20.").


216. See, e.g., Fon & Parisi, supra note 208, at 149 ("The lack of a perfect fit between the ex ante legal rule and the circumstances of individual cases may create social losses. From an efficiency perspective, standards allow ad hoc custom-tailoring of the law to the circumstances of the case at bar, reducing problems of over-inclusion and under-inclusion."); see also John Braithwaite, Rules and Principles: A Theory of Legal Certainty, 27 AUSTL. J. LEGAL PHIL. 47, 60–75 (2002) (showing, based on a comparative study of the regulation of nursing homes in the United States and Australia, how a regulatory regime based on the proliferation of detailed rules creates an unwieldy, confusing body of rules and exceptions, leading to uncertain and inconsistent applications).


218. Id.

imperfect proxy for the rule-maker’s intended purpose” out of a need for administrability.220

In these ways, the process of technological translation of legal mandates governing risk management encounters a “many hands problem.”221 At any number of steps, it can incorporate decisionmaking biases reflecting the analytic limits of business, legal, and technological logic, as each translator attempts to corral the notion of risk through its own system of legitimacy. If one “consequence of modernity” is that no expert system can be wholly authoritative in the consequences of its expert principles,222 the phenomenon is compounded by the interaction of multiple expert systems, each lacking the concomitant ability to oversee fully the language brought to bear by the others.

2. Systemic Effects.—Once bias is introduced into technology systems, the resulting shortcomings can prove particularly sticky and resistant to detection or repair. To be sure, the purveyors of technology solutions tout their plasticity—223—the ability to reshape and adapt code as circumstances demand. Yet while significant “latitude of choice exists the very first time a particular instrument, system, or technique is introduced,” flexibility largely vanishes once the “initial commitments” are made.224 Such path dependence transforms it, in the words of one socio-technical scholar, from a device “oriented toward human needs” into “an important component[] of the formative context.”225 This characteristic, too, tracks code’s function as law:

220. Id. at 194; see also Roger Brownsword, So What Does the World Need Now? Reflections on Regulating Technologies, in REGULATING TECHNOLOGIES: LEGAL FUTURES, REGULATORY FRAMES AND TECHNOLOGICAL FIXES 23, 44 (Roger Brownsword & Karen Yeung eds., 2008) (“[F]or whatever traditional legal rules might mean on paper, there is often a practice around the rule that is quite different.”).

221. See Helen Nissenbaum, Accountability in a Computerized Society, in HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY 41 (Batya Friedman ed., 1997) (discussing the ways in which the “problem of many hands” erodes accountability in computerized societies); see also Claudio U. Ciborra, De Profundis? Deconstructing the Concept of Strategic Alignment, 9 SCANDINAVIAN J. INFO. SYS. 67, 77 (1997) (“[O]ne can take for granted that management can in various degree harness IT infrastructure to achieve business goals . . . . However, a closer look at the internal dynamics of IT infrastructure would show that: many actors are involved in its establishment or development, so that it is not controlled by only one actor.”).


223. See, e.g., Grimmelmann, supra note 102, at 1730–31 (quoting FREDERICK P. BROOKS, JR., The Tar Pit, in THE MYTHICAL MAN-MONTH 3, 7 (anniversary ed. 1995) (1975) (“Few media of creation are so flexible, so easy to polish and rework, so readily capable of realizing grand conceptual structures.”)).


225. Ciborra, supra note 221, at 76; see id. at 76–77 (arguing that while people initially create technological infrastructures to serve their particular needs, ultimately this very infrastructure has as great of an influence in shaping human behavior as the humans had in shaping it).
technology is "similar to legislative acts or political foundings that establish a framework for public order that will endure over many generations."226

This systematization of initial patterns persists for technical, institutional, and cognitive reasons. While computer code and predictive-analytic methods might be accessible to programmers, they remain opaque to users—for whom, often, only outcomes remain visible.227 Programmers "code[] layer after layer of policies and other types of rules" that managers and directors cannot hope to understand or unwind228—a phenomenon exacerbated by the prevalence of off-the-shelf GRC products and risk analytics. Furthermore, "[t]he ability to [understand] complex financial instruments requires literally a Ph.D. in applied mathematics."229 Not surprisingly, in a recent survey of directors of public companies, only 5.4% of the respondents rated their "board's ability to monitor a risk management plan to mitigate corporate exposure" as "very effective."230

3. Cognitive Bias in Decisionmaking.—The opacity of the underlying metrics contributes to risk technology's ability to shape what Heidegger called a "world view" or "frame."231 In the case of GRC systems, this representational power of technology claims a literal manifestation, as managers and officers sit before "executive dashboards," which indicate "automatically" and "comprehensively" whether problematic levels of risk exist or whether they do not.

The power of such representations can, however, come at a cognitive cost. Human judgment is subject to an automation bias, which fosters a ten-
endency to "disregard or not search for contradictory information in light of a computer-generated solution that is accepted as correct."232 Such bias has been found to be most pronounced when computer technology fails to flag a problem. In a recent study from the medical context, researchers compared the diagnostic accuracy of two groups of experienced mammogram readers (radiologists, radiographers, and breast clinicians)—one aided by a Computer Aided Detection (CAD) program and the other lacking access to the technology. The study revealed that the first group was almost twice as likely to miss signs of cancer if the CAD did not flag the concerning presentation than the second group that did not rely on the program.233 Moreover, the bias is more salient when the computer-prompted result comports with the financial interests of the decisionmaker. Behavioral studies, for example, find that automation of financial fraud controls increases complaisance in oversight by those corporate actors charged with compliance, skewing individual decisions towards those that maximize personal earnings.234 Thus, the benefits of machine "judgment" may come at the cost of human decision-making effectiveness, especially when the goals embodied by technology systems create tension with other powerful organizational or individual incentives.

More generally, existing understandings of risk and how it should be measured become institutionalized, drawing even more attention away from less easily quantifiable—although perhaps more essential—uncertainty that is left off the screen. Such institutionalization might permit evolutionary improvements in existing risk measurements, but it masks areas where risk types are ignored or analysis is insufficient and where more revolutionary, paradigm-shifting advances might be warranted.235

These understandings (or misunderstandings), finally, can be institutionalized across the field of risk management. As risk assessment and legal-compliance practices are disseminated through the industry by professional groups, risk-management practitioners, management scholars, and third-party technology vendors and consultants, they standardize an approach


235. See Scheytt et al., supra note 205, at 1333 ("If partial explanations of events which suit interested parties become institutionally accepted as legitimate, organizational reform processes may follow a logic which increases rather than decreases risk.").
that other firms adopt, seeking legitimacy. This process of institutional isomorphism can formalize myths about the rationality, efficacy, and legal sufficiency of dominant practices—myths that legal actors, too, may adopt. Isomorphism can thus foster systemic vulnerability by eliminating variety in risk measures and outlooks across an entire industry. Such homogeneity, which can render an entire sector susceptible to a single type of risk-assessment failure, is especially harmful in contexts where robustness depends on diversification as a hedge against exogenous risk events.

By these phenomena of representation and institutionalization, technology systems, developed to manage risk, in turn, become sources of risk themselves. They create the perception of stability through probabilistic reasoning and the experience of accuracy, reliability, and comprehensiveness through automation and presentation. But in so doing, technology systems draw organizational attention away from uncertainty and partiality. They can embed, and then justify, self-interested assumptions and hypotheses. Moreover, they shroud opacity—and the challenges for oversight that opacity presents—in the guise of legitimacy, providing the allure of shortcuts and safe harbors for actors both challenged by resource constraints and desperate for acceptable means to demonstrate compliance with complex and unwieldy legal mandates and market expectations. Technology systems, accordingly, create the systemic preconditions for the integral

---

236. See Paul J. DiMaggio & Walter W. Powell, The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields, 48 AM. SOC. REV. 147, 152 (1983) ("Organizations tend to model themselves after similar organizations in their field that they perceive to be more legitimate or successful."); W. Richard Scott & John W. Meyer, The Organization of Societal Sectors, in ORGANIZATIONAL ENVIRONMENTS: RITUAL AND RATIONALITY 129, 140 (John W. Meyer & W. Richard Scott eds., 1983) ("Institutional sectors are characterized by the elaboration of rules and requirements to which individual organizations must conform if they are to receive support and legitimacy from the environment.").

237. See Lauren B. Edelman et al., The Endogeneity of Legal Regulation: Grievance Procedures as Rational Myth, 105 AM. J. SOC. 406, 416 (1999) (contending that, in the context of grievance procedures, "myths [of rationality] originate from models that have already been institutionalized in other social arenas...[that] influence law and, hence, market forces"); Lauren B. Edelman et al., Internal Dispute Resolution: The Transformation of Civil Rights in the Workplace, 27 LAW & SOC’Y REV. 497, 529 (1993) (characterizing organizational complaint handlers' approaches to handling discrimination complaints as "[subsuming] law within the managerial realm...[and] transforming [law] into a diffuse standard of fairness"); cf. JANET M. TAKAVOLI, DEAR MR. BUFFETT: WHAT AN INVESTOR LEARNS 1,269 MILES FROM WALL STREET 38 (2008) (quoting an internal Berkshire Hathaway memo from Warren Buffett as reading, "The five most dangerous words in business may be 'Everybody else is doing it'.").

238. See Scheytt et al., supra note 205, at 1333 ("Stable climates of probabilistic reasoning in risk management are challenged by the transformation of side-effects into new risk 'objects'..."").

239. See BARDACH & KAGAN, supra note 37, at 64–66 (arguing that most regulated enterprises are "good apples" that wish to comply with regulation); see also J.B. Ruhl & James Salzman, Mozart and the Red Queen: The Problem of Regulatory Accretion in the Administrative State, 91 GEO. L.J. 757, 805 (2003) (describing the problem of regulatory accretion, whereby the "system burdens" arising from the collective operation of rules thwart a regulated organization's ability to comply).
accident—the notion that “the invention of the ‘substance’ is equally invention of the ‘accident.’”

4. Opportunities for Gamesmanship.—Finally, these elements of technology systems can facilitate the gaming of those very systems by actors within the regulated organizations they are intended to govern. Internal organizational incentive structures, especially in industries generating the types of instability policy makers seek to reduce, frequently reward the type of abnormal successes that can arise from undesirably risky behavior. The predictability of rule-bound code and the often static nature of technological implementations can permit individual actors motivated by organizational incentives and individual greed to manipulate their behavior in ways that mask its riskiness from technological sensitivity. Layers of technological opacity, moreover, can shield such behavior from both internal and external oversight until negative outcomes manifest themselves. Thus, systems intended to identify exceptions can, in the hands of those familiar with them, serve to shield remarkable behavior.

C. Technology Pitfalls on the Ground: Illustrative Cases

The effects of different combinations of these phenomena—albeit with implications of varying severity—can be seen in two very different experiences: compliance with information-privacy regulation on one hand, and regulation of risk in financial institutions on the other.

1. Case 1: Technology Limits and Information Privacy.—Information-privacy regulation in the United States is most often identified with discrete, sector-specific statutory schemes governing the treatment of personally identifiable information, such as HIPAA, the regime governing data in the health sector. In these contexts, computer scientists have achieved successes in developing technology systems that “reduce[s] high-level [legal requirements and societal expectations] to specific operating guidelines that can be applied

240. PAUL VIRILIO, THE ORIGINAL ACCIDENT 5 (2007); see also id. (“The shipwreck is consequently the ‘futurist’ invention of the ship, and the air crash the invention of the supersonic airliner, just as the Chernobyl meltdown is the invention of the nuclear power station.”); CHARLES PERROW, NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES 3–5 (1984) (asserting that complex technological systems will inevitably fail and therefore produce “normal accidents”).


243. See supra notes 51–54 and accompanying text (discussing the regulations and requirements associated with HIPAA).
Technologies of Compliance

at individual steps in a business process or organizational workflow. Sophisticated HIPAA compliance systems can model workflows in ways that maximize both privacy and utility; control access to prevent inappropriate viewing by particular types of workers or inappropriate combination of types of data; and use auditing algorithms and heuristics to flag suspicious actions. Across sectors, moreover, firms increasingly rely on privacy-enhancing technologies (PETs), technological measures intended to “translate ‘soft’ legal text into ‘hard’ system specifications.” These systems seek principally to “anonymize” data by stripping it of what are characterized as personally identifiable characteristics, in order to enforce privacy protection “without the loss of the functionality of the information system” itself.

Recent developments, however, have revealed at least two types of limits to such systems.

The first arises from the choice of which legal requirements to “translate” into “hard system specifications,” the institutionalization of those choices, and the manner in which they narrow institutional focus. As Professor Deirdre Mulligan and I explore elsewhere, the comparative importance of discrete, and relatively static, statutory requirements in privacy compliance has diminished. The privacy space has instead been enhanced by a more fluid and dynamic understanding of the legal requirements of privacy protection. In large part, this enhancement comes as the result of robust enforcement activity by the Federal Trade Commission and State Attorneys General pursuant to their broad-reaching consumer-protection powers.

As a result, legal privacy requirements have increasingly expanded beyond procedures that can be reflected in actionable, and codifiable, rules. The law instead progressively reflects the notion that market actors should adopt privacy protections informed by “consumer expectations” regarding

245. See id. at 292–93 (deriving a general theory of how compliance systems can be used effectively to promote HIPAA compliance, in part by reference to the important work done on the MyHealth@Vanderbilt web-based patient portal built and used at the Vanderbilt Medical Center).
247. See id. at 34 (“PET stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system. PET incorporated systems use Identity Protectors and divide systems into identity, pseudo-identity and anonymity domains.” (citation omitted)).
the appropriate treatment of individual information and personal identity—a standard that requires judgment in its implementation because it both evolves and varies by context.249

Dominant-access control and privacy-policy frameworks, however, do not reflect such a contextual understanding of privacy, which require much more sophisticated modeling of “who personal information is about, how it is transmitted, and past and future actions by both the subject and the users of the information.”250 Thus pervasive claims by technology developers to provide “comprehensive” privacy-compliance-technology solutions251 through PETs relying on actionable rules, can draw organizational attention away from these technologies’ limits as full compliance tools.252

The second constraint faced by such technology systems arises from the institutionalized agreement as to appropriate measures necessary for privacy protection, and the systems’ resulting stickiness and resistance to vulnerability detection or repair. While it has become a commonplace that anonymization tools offer a central pillar to a privacy protection regime,253 such consensus has overlooked evidence that the effectiveness of current methods for “anonymizing” data (i.e., the removal of certain personally identifiable information) has been significantly overestimated.254 As a result, technologically sophisticated parties such as AOL, Inc., and Netflix, Inc., which relied on such standard techniques, ended up ignoring the risk that information could be “reidentified,” leading to significant, and very visible, privacy breaches, as their customers’ search queries and movie rental histories were reconstructed publicly.255

249. See generally HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE 2–3 (2009) (describing the importance of context in determining whether information is used appropriately, and therefore for meaningful privacy protection).


2. Case 2: Technology Failures and the Financial Crisis.—Even more strikingly, these phenomena lay at the heart of the recent financial crisis. In recent years, loan originations and valuations—including those involving the mortgages that would later spur early manifestations of crisis—were increasingly automated. Additionally, corresponding assessments of risk were increasingly tacked to analytics with certain embedded hypotheses, including flawed assumptions about the future of housing markets. Standard securitization models, moreover, made numerous assumptions about the risk of default or delinquency before repackaging a collection of loans into asset-backed securities, or collateralized debt obligations (CDOs), which were then used as collateral against further loans.

The unregulated, and nonstandardized, nature of the complex derivative products to which financial institutions increasingly turned as vehicles for hedging risk—including the risk of structured investment vehicles like CDOs—further centralized the criticality of systemic analytics. While sellers of derivative contracts like credit-default swaps (CDSs)—in which one party bets on the failure of an underlying financial instrument by making periodic payments in exchange for the chance to receive a payoff in case of default—were not required to maintain any reserves to pay off buyers, all major CDS dealers were subject to bank capital requirements. For these purposes, they needed to value CDSs based on computer modeling of the risk of default in the underlying debt. Yet, as CDSs were issued for highly leveraged and increasingly uncertain derivative products, these

256. See Marsha Cochrane et al., Industry Changes in the Market for Mortgage Loans, 41 CONN. L. REV. 1143, 1153 (2009) (listing automated underwriting tools as one of several recent innovations in the mortgage market).


261. See id. at 56 (asserting that even securities firms, which are typically held to lower requirements than banks themselves, are still subject to the capital requirements if they are owned by a bank or financial holding institution).

262. See Brady Dennis & Robert O’Harrow Jr., Financial Crisis: Complex Deals Veiled Risk for AIG, L.A. TIMES, Jan. 1, 2009, at C1 (describing how AIG relied on a consultant computer model that calculated risks when it began investing in credit-default swaps in 1998 and how the model projected a “99.85% chance of never having to pay out”—so remote “that the fees were almost free money”).
investments often no longer had a known entity to follow in determining the strength of a particular loan or bond (as in the case of CDSs for commercial loans, corporate bonds, or municipal bonds).\textsuperscript{263}

These developments posed formidable challenges for risk management. Through this process, financial institutions faced the need to arrive at point estimates for the value and risk of new types of mortgages, engineered securities, and debt-hedging contracts in order to comply with reserve and capital requirements.\textsuperscript{264} Accordingly, they sought to stretch analytics embedded in established risk-management systems to new contexts. In particular, financial institutions applied the technological systems institutionalized for calculating the short-term risk of traditional financial holdings—and the VaR approaches on which they relied—to calculate the level of risk inherent in the unregulated CDO and CDS markets.\textsuperscript{265} VaR methodology was originally developed as a means for identifying optimal portfolios for equity investors, based on both market risks and the interrelation between, or “co-movements” of, such risks.\textsuperscript{266} It was integrated after the 1987 stock-market crash as a means for commercial and investment banks to capture the potential loss in value of their traded portfolios from adverse market movements over a specified period.\textsuperscript{267}

VaR measures involve three elements: (1) the potential loss in value of a risky asset (2) over a defined period (3) for a given confidence interval.\textsuperscript{268} Thus, if the VaR on an asset is $100 million at a one-week, 99% confidence level, it means that there is a 1% chance that the value of the asset will drop more than $100 million over any given week. Generally, VaR approaches reach their calculation by mapping the range of possible loss outcomes and their probabilities for each asset. These probabilities are reached by a variety of calculation methods, notably (1) integration of calculations of the variance of a type of asset with those of covariances across different kinds of assets,\textsuperscript{269} and (2) those that use what are called Monte Carlo simulations—an approach useful in studying systems with a large number of connected but independent elements (such as scientific phenomena like fluids and cellular structure)—which simulate the multiple sources of uncertainty affecting an asset’s value,

\textsuperscript{263} See id. (explaining that private CDSs allowed a greater amount of financing and leveraging than regulators allowed for publicly traded debt).

\textsuperscript{264} Benton E. Gump & Thomas Lutton, Potential Effects of Fair Value Accounting on US Bank Regulatory Capital, 19 J. APPLIED FIN. 38, 39 (asserting that Federal Accounting Standards Rule 157—now recodified at ASC Topic 820—requires point estimates).

\textsuperscript{265} See, e.g., Dennis & O’Harrow, supra note 262 (describing the computer program AIG used to calculated the risk of CDSs).


\textsuperscript{268} Adrogué, supra note 266, at 67.

\textsuperscript{269} Id.
and then aggregating the results of a large number of possible outcomes. Critically, both of these methods generally draw on historical data for their distributional assumptions.

VaR embodied the promise of technology systems for risk management, and it was disseminated quickly. In 1995, JP Morgan, which largely pioneered development of the method in the financial context, coined the term and provided public access to its internal data on the variances of, and covariances across, various security and asset classes, allowing software engineers to develop risk-measurement programs. These would provide the technological basis for what former JP Morgan CEO Dennis Weatherstone called the "4:15 report"—a one-page firm risk report available 15 minutes after the market’s close.

When the SEC required, in 1997, disclosure of quantitative information regarding public-company derivatives activity, the agency specifically listed VaR as an acceptable method for calculation. And as legal risk-management mandates proliferated and risk complexity deepened, VaR proved an especially attractive risk-valuation model for two reasons. It provided a means for attaining a particularized measure for things that could not be predicted directly; and, it became the only common risk measure that could be defined for any type of risk, which permitted the comparison and aggregation of measures necessary for enterprise-wide risk management and reporting. VaR was accordingly institutionalized as a foundation of the specialized risk-management analytics developed by large financial institutions and included in GRC technology offerings geared towards compliance with Basel II and other financial regulation.

Over time, however, the breadth of activity to which VaR analysis was applied widened. VaR had developed during the technological transformation of trading from the floor to a culture of individual traders sitting across


271. See id. at 294 (criticizing the various VaR models' reliance on previously observed correlations).


276. JORION, supra note 273, at 71–74.
from computer screens—those whose valuations can be grounded in prices quoted on markets. Yet, increasingly, systems rooted in VaR approaches were called on to calculate the risk posed by long-maturity assets—assets whose value was tied not to market data, but to nonobservable assumptions, either by analogy to other assets or through financial modeling. These assessments, in turn, would serve as the means for identifying what types of internal controls should be implemented and triggering the level of capital reserves necessary for legal compliance.

Moreover, as analytics became more speculative, reliance on the technological controls developed in their light often crowded out more subjective human inputs. As Professor John Coffee explains:

Most of the investment banks used to do due diligence in asset-backed securitizations by hiring professional due diligence firms with expertise in real estate to test the loan originator’s portfolio of mortgages before the bank acquired its loans. They began to abandon that practice after 2002, as the market became more bubbly and demand for these deals grew and grew.

Perhaps more shockingly, in the six months before its meltdown, AIG did not have either a full-time CFO or chief risk-assessment officer. Bear Stearns, too, lost its top risk modeler “precisely when the subprime crisis was beginning to hit” and conducted neither periodic evaluations of its VaR models nor timely updates of inputs to its VaR models. Indeed, according to the findings of the SEC’s Inspector General, given their “lack of expertise in mortgages, it would have been difficult for risk managers at Bear Stearns to advocate a bigger focus on default risk in its mortgage models.” And, at the same time, traders were permitted to game VaR measures by “stuffing risk into the tails”—that is, making investments that pose only an extremely

278. FAIR VALUE MEASUREMENTS, Accounting Standards Codification Topic 820-10-35 (Fin. Accounting Standards Bd. 2009).
279. See Nocera, supra note 1, at 26, 28–29 (contending that VaR was unable to accurately gauge the risk of mortgage-backed securities because VaR is based on a limited two-year data history); cf. The Risks of Financial Modeling: VaR and the Economic Meltdown: Hearing Before the Subcomm. on Investigations & Oversight of the H. Comm. on Science & Technology, 111th Cong. 5–6 (2009) (statement of Christopher Whalen, Managing Director, Institutional Risk Analytics) (arguing that Wall Street used the “alchemy of financial modeling” to create and hide risk).
283. Id.
small risk of very large losses, meaning that those “losses lie in the ‘fat tail’ of a loss curve and outside a value-at-risk measurement.”

The collapse of the housing market revealed the profound shortcomings of these analytics and of overreliance on risk-management technology at the expense of human judgment. The institutionalization of increasingly complex programming offered a promise of certainty and precision that obscured profound uncertainties that VaR models cannot accurately capture. Assumptions used to assign outcome probabilities were informed by historical-trend data that often began at the 1987 stock-market crash and overemphasized the subsequent rise in housing and capital markets. VaR, moreover, is not geared to identifying gap risk—the risk of extreme market events that fall outside of the 95%- or 99%-likely probabilities it defines. Especially to the extent that VaR models assume normal probability distributions of these unlikely events, the extreme risks they pose will be discounted under the static, and originally short-term-focused, VaR-risk-measurement approach. In particular, VaR does not capture the import of such uncertainty over long time periods; the impact on potential losses of particular characteristics of structured-credit products—such as their limited liquidity and the “non-linearity” of their risk (basically, the fact that all tranches of mortgage-backed CDOs would either hold or lose value together); or other systemic factors like credit-rating risk.

Despite these underlying failures, however, until the point of systemic collapse, risk-assessment technologies that were directed towards control obscured oversight at every level. Financial technology’s ability “to quantify

284. Gerding, supra note 241, at 179–80 (quoting Nocera, supra note 1, at 46). See generally RENE M. STULZ, RISK MANAGEMENT AND DERIVATIVES 621 (2003) (explaining that VaR can be biased not only because of “implementation problems” but also “for a more fundamental reason if we are assuming the wrong distribution for the portfolio return”).

285. See Taleb, supra note 33.

286. See Rob Jameson, How the Risk Models Failed the World’s Banks: Why Didn’t the Banking Industry Foresee the Crisis that Afflicts It?, NEW SCIENTIST, Sept. 27, 2008, at 8, 9 (observing that because risk-analysis systems only used recent U.S. data, they were unable to recognize the catastrophic effect that a nationwide downturn in housing prices would have on the banking system); Nocera, supra note 1, at 28–29 (noting that Black Monday, Oct. 19, 1987—the date of the largest one-day stock-market-percentage decline in history—has been used as a worst-case scenario in many risk models and observing that risk analysis based on the culmination of the housing bubble in 2005–2006 was inadequate to predict what happened to the markets in 2007–2008).

287. VaR is thus geared towards measuring “Knightian risk,” which involves situations where probabilities are given. VaR is not geared towards “Knightian uncertainty” (which refers to situations in which possible outcomes can be identified but probabilities are not measurable), FRANK H. KNIGHT, RISK, UNCERTAINTY AND PROFIT 19–20 (1921), or towards situations involving “structural ignorance” (where outcomes are neither naturally given nor easily constructed by the decisionmaker), ITZHAK GILBOA & DAVID SCHMEIDLER, A THEORY OF CASE-BASED DECISION 45 (2001).

288. See Gerding, supra note 241, at 141 (explaining that, in order to calculate VaR, modelers must and do make one of three assumptions: that the distribution of risk is normal, that it is based on historical patterns, or that it follows the prediction of a Monte Carlo simulation).
the immeasurable with great precision289 permitted regulated firms to present regulators with quantitative evidence of compliance with risk-management mandates and capital-reserve requirements—especially after those obligations were reduced by the SEC in 2004.290 Technology systems skewed internal and external controls in ways that masked manipulative behavior by those whose short-term incentives pushed towards unreasonably risky behavior (the financial-products division of AIG, whose actions led to the insurer’s loss of $11.5 billion, worked with models calculating a 99.85% chance that AIG would never have to pay out on the CDSs it executed,291 while the credit-rating agencies’ ultimate downgrading of AIG’s AAA rating to AA was completely unrelated to these products). Finally, such technology masked the true nature of risks even to the directors and officers mandated to manage them. A confidential review ordered by then-New York Federal Reserve Board President Timothy Geithner in 2006 found that banking companies simply could not properly assess their exposure to a severe economic downturn.292 Meanwhile, former SEC Chair Harvey Goldschmid has explained more recently that “even at senior levels [at the Wall Street investment houses] they only vaguely understood the risks.... And when it tumbled, there was some genuine surprise not only at the board level where there wasn’t enough oversight but at senior management level.”293

V. Governance Implications

If code shapes legal meaning through implementation of formal mandates, this account makes clear that private-firm reliance on technology systems can, in predictable ways, make bad law. While technological controls offer powerful tools for enabling organizational actors to achieve regulatory goals, they can in turn shape organizational decisionmaking in

289. Taleb, supra note 33.
291. Robert O’Harrow Jr. & Brady Dennis, A Crack in the System, WASH. POST, Dec. 30, 2008, at A1. The computer models developed by Yale University business professor Gary Gorton forecasted that the only scenario in which AIG would have to pay out was in the case of a full-blown depression, in which case the counterparties would go bankrupt and would not likely demand payment. Id.; see also American International Group, Annual Report (Form 10-K), at 129 (Dec. 31, 2007) (“AIG did not maintain, in all material respects, effective internal control over financial reporting ... because a material weakness in internal control over financial reporting related to the AIGFP super senior credit default swap portfolio valuation process and oversight thereof existed as of that date.”).
ways that drift significantly from those ends, raising issues of both effective governance and legitimate public administration.

Yet, if administrative reticence provides insufficient bulwarks against effective implementation, what would a more-involved model of regulator involvement entail? What should be the primary concerns in a compliance setting when dealing with shortcomings that plague the deployment of technology generally? What governance values are most at peril? What values must be balanced in seeking policy responses? And what mechanisms might a more-involved regulatory model deploy in addressing these concerns?

A. Framing Technology Accountability

In beginning to answer these questions, it is useful to consider what scholars have called “regulating” technologies—technology that embeds behavioral and decisional constraints of interest to law—in at least a few other contexts. The development of a comprehensive typology of “normative” technologies falls well beyond the scope of this Article. Yet a brief consideration of compliance technology’s place in this larger category can both help identify the contours of the concerns that attach to “technologies of compliance” in particular, and suggest directions for sketching out solutions.

Such regulating technologies, as a category, reflect the general characteristics of what might, in Lessig’s terms, be called “architectural” technology: the background technical standards and protocols—or code—that define the technological “place” in which human behavior occurs. Such digital architecture constrains human behavior in ways that can compete with, and substitute for, legal regulation. Yet, unlike legal regulation, it can present a particular type of deep opacity. Embedded values can remain hidden, and the forces that shape those choices, whether governmental, social or market, are often shrouded. Indeed, the fact that

294. E.g., Roger Brownsword & Karen Yeung, Introduction to REGULATING TECHNOLOGIES: TOOLS, TARGETS AND THEMATICS, supra note 220, at 7, 13 (distinguishing between legal issues arising from the use of technology as a “regulatory tool” and those involved with technology as a “regulatory target”).


296. More synthetic accounts of technological functionalities and potential regulatory responses can be found, for example, at Jay P. Kesan & Rajiv C. Shah, Shaping Code, 18 HARV. J.L. & TECH. 319 (2005) and Koops, supra note 295. See also Reidenberg, supra note 31, at 588–91, for an examination of ways in which public policy can change code.

297. LESSIG, supra note 31, at 341–45.

298. See JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 153 (2006) (“Technologies of control designed to serve legitimate and desired ends can rarely be limited to those ends, and will often be co-opted for illegitimate purposes.”). The more important lesson is that the Internet is not, as many in the 1990s believed, “an unstoppable juggernaut that will overrun the old and outdated determinants of human
architectural technology embodies normative choices at all can escape notice, as the perfect constraints code places on behavioral possibility can seem as natural, immutable, and invisible as the laws of physics. Such indirect regulation therefore easily evades the usual social and political processes that shape the normative choices reflected in direct regulation—public and open debate, elections, and policy making within a representative structure. It is, therefore, to these modes of accountability and legitimacy—participation, deliberation, and democracy—to which many scholars turn in conceiving of policy responses.

Technologies of compliance, however, present a particular type of architectural constraint in two ways. First, while many types of technology shape behavior by function of their use, compliance technology constrains decisions intentionally. Second, their intent is to embody norms decided upon elsewhere—in this sense they are purportedly norm enforcing rather than norm setting.

Thus while the sophisticated literature on technology as an architectural regulator offers important general insights as to the value-laden nature of technological choices and the ways in which they can shape the perceptions of users, the norm-enforcing character of compliance technology suggests that any accountability concerns it raises do not arise principally out of a broad-based disconnect from democratically legitimate law-elaboration processes. For in the compliance context, first principles have already been determined through constitutionally valid congressional and administrative identification of public priorities and policy goals, along with decisions about the enlistment of regulated firms in their achievement. Rather, it suggests that governance concerns would arise from any practical divergence between those norms “on the books,” and their implementation, both in the code itself, and in the human interactions with it.

Helpful suggestions regarding particular manifestations of such governance concerns have been identified by scholars in at least two other contexts. The first involves technology intended to enforce private intellectual property rights. Such “technological protection measures” are typified by Digital Rights Management (DRM) software created by private parties organization." Id. at 183. To the contrary, the Internet itself is taking on the characteristics—good and bad—of the governments and people beneath it in different parts of the world. See id. at 184 (“[T]he openness of the network is contingent, and one of the most important things it is contingent on is governmental coercion that demands a unique architecture.”).

299. See Koops, supra note 295, at 158 & n.2 (noting that all technology inherently “has a regulatory effect on people’s behavior” but arguing that the crucial innovation in normative technology is that it “contains intentionally built-in rules”).

300. Cf. id. at 159 (noting that the broader category of normative technology includes both “norm-establishing” and “norm-enforcing” incarnations).

Technologies of Compliance

and embedded in digital-content files for sale or distribution.  

This intentionally-norm-enforcing technology then governs the way those files can be used and shared. Specifically, DRM is intended to make obligatory rights and agreements protected by existing property and contract law. Yet certain attributes of its operation undermine the contours of that law in troubling ways. The private production of these technologies creates the possibility that public goals can be subverted by parties with an incentive for overprotection of property rights. Specifically, the regulatory capacity of rule-based code creates the possibility for perfect constraints on use in a way unanticipated by law, which by contrast admits for "fair use" exceptions to pure copyright protection. Because fair use "inherently requires a judgment about purpose, or intent," DRM's technological constraints crowd out subjective, human elements of legal enforcement, which are "beyond the ken of even the best computers." DRM, moreover, also poses a type of opacity problem—this time a practical opacity—in that most consumers lack the necessary expertise to understand its "complex technical terminology" or the bargaining power to negotiate a change. These factors disable market constraints on the development of technological standards consistent with free private ordering of rights allocation and protection. In response, various scholars suggest the involvement of other actors who can bring different viewpoints and incentives to technological decisionmaking, from government regulators who could certify that technological protection measures contain back doors for the incorporation of public norms, to trusted third

302. See LESSIG, supra note 31, at 116 (describing DRM, such as Apple's "fairplay" encoding of iTunes songs, as technologies that "add code to digital content that disables the simple ability to copy or distribute that content—at least without the technical permission of the DRM technology itself").

303. For example, from 2006 until 2007, Sony BMP sold CDs containing covert DRM software that embedded itself on a user's computer. The software created security vulnerabilities, completely blocked the user's ability to copy music, and reported personal information about the user back to Sony—all with no notice to the user. Once discovered, Sony was charged with various deceptive trade practices and eventually consented to a settlement with the FTC allowing users to exchange all of the sold CDs, provide clear labeling of all future DRM software on CD packaging, and reimburse consumers for damages to their computers. Press Release, FTC, Sony BMG Settles FTC Charges (Jan. 30, 2007), available at http://www.ftc.gov/opa/2007/01/sony.shtm. See generally Deirdre K. Mulligan & Aaron K. Perzanowski, The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident, 22 BERKELEY TECH. L.J. 1157, 1165 (2007) (discussing "the market, technological, and legal factors that appear to have led a presumably rational actor [Sony] toward a strategy that in retrospect appears obviously and fundamentally misguided").

304. See generally 17 U.S.C. § 107 (providing for copyright's fair-use exception).

305. LESSIG, supra note 31, at 187.


parties who would hold in "escrow" a key to the DRM code and could, where appropriate, permit low-cost or free fair use of content.\(^{308}\)

Thus, these sorts of control technologies suggest a suite of accountability concerns: opacity in technological operation, skewing of public legal norms by private interests, and the subversion of subjective human judgment where it had traditionally been important to legal implementation. Faced by the failure of legal or market constraints to protect such values, legal scholars have, in turn, suggested the need for the development of external institutions that can foster accountability in technology choices.

A related suite of accountability concerns has been identified where technology is employed in the operation of government functions previously accomplished in other ways. Examples include the adoption of electronic voting machines\(^{309}\) and technology systems that administer eligibility for public benefits.\(^{310}\) In these contexts as well, technology is utilized in an effort to implement existing norms more effectively and efficiently. Thus, here efficacy, accuracy, and reliability are paramount, yet each of these representative data-management systems has suffered notorious instances of failure. These particular malfunctions have been traced, in part, to a different variety of opacity—one that also implicates concerns of privatization. In each instance, either because the systems’ software is proprietary or shielded as a matter of public policy, the source code is secret.\(^{311}\) Thus even though the functions involved are traditionally those of a public actor, the management of those functions is private. Such closed-source code leaves outsiders “unable to discern how a system operates and protects itself”\(^{312}\) and shields unintended errors that distort even clear legal and managerial goals.

In this context, the accountability rubric largely focuses on transparency and oversight—the “opening” of code—so as to facilitate two types of accountability: first, review by experts of the mechanisms of public administration; and second, review by courts considering arguments that the

---


310. See Citron, *supra* note 204, at 1260–67 (describing the design, implementation, and hurdles of automated-decision systems used for public-benefit programs such as Colorado’s state benefits, the Food Stamp Act, and the National School Lunch Program).

311. See Citron, *supra* note 309, at 357 (“Because these systems’ software is proprietary, the source code—the programmers’ instructions to the computer—is secret.”).

312. *Id.*
adoption of technological management so alters the substantial operation of
government that it threatens the constitutional protections of its citizens.313

Considering technology's compliance functionality in light of these
other scenarios casts into sharper relief the accountability concerns technol-
ogy systems may raise and mechanisms for response. The suite of concerns
from the private-rights enforcement and management contexts resonates
strongly here. Concern about the ways private incentives can subvert public
norms is paramount in the compliance context, albeit manifest in varying
ways. In the privacy-compliance context, for example, regulation requires
the integration of a system of protective controls—controls that firms would
likely not develop on their own—into existing information systems organized
around the maximization of a competing goal: the utility of privately held
data to the firm. In the financial-institutions context, by contrast, regulation
seeks to co-opt an already pervasive private risk function for public (yet
loosely defined) ends. In both, the interests of the actor developing the tech-
nology might diverge significantly from those of the public regulator.

Furthermore, the technical language of compliance systems obscures the
accountability of the decisions they channel. Programming and mathematical
idiom can shield layers of embedded assumptions from high-level firm
decisionmakers charged with meaningful oversight314 and can mask impor-
tant concerns with a veneer of transparency. This problem is compounded in
the case of regulators outside the firm, who frequently lack the resources or
vantage to peer inside buried decision processes and must instead rely on the
resulting conclusions about risks and safeguards offered them by the parties
they regulate.

Perhaps a concern salient in the compliance context even more than the
others, moreover, is the importance of the sound exercise of human judgment
and of ensuring that technology supports, rather than obscures, that goal.
The compliance context requires that accountability focus on discretion and
its exercise. To be sure, judgment plays a varied role in technologies of
compliance; some systems, such as those that focus on comprehensive
storage (of all e-mails, for example), or tracking (such as every log-on or log-
off from a computer system), demand little discretion. But, as the level of
judgment required increases—from decisions governing how to sort and

313. See, e.g., Citron, supra note 204, at 1258, 1278–1300 (arguing that automated benefits-
management systems jeopardize due process norms); see also Erin Murphy, Paradigms of Restraint,
57 DUKE L.J. 1321, 1393–1411 (2008) (arguing that governmental substitution of technological for
physical systems for restraint of dangerous persons merits constitutional scrutiny).

responsibility for U.S. public-company boards); In re Caremark Int'l Derivative Litig., 698 A.2d
959, 970 (Del. Ch. 1996) (stating that a director's obligation includes a duty to attempt in good
faith to assure that a corporate information and reporting system, which the board concludes is
adequate, exists," and that it is impossible for directors to satisfy their obligation to be reasonably
informed about the corporation's operations without doing so).
characterize data, to rules constraining its use, to analytics deriving meaning and predictions, to rules automating decisions accordingly—accountability measures must increasingly promote its exercise. For as a general rule, technology-based compliance systems proliferate in contexts in which policy makers have rejected rule-based mandates in favor of regulatory principles that rely, for their implementation, on the exercise of context-specific judgment by regulated entities. Yet compliance technology can turn each of these regulatory choices on its head. The need to translate both legal and management concerns into a third distinct logic of computer code and quantitative analytics creates the possibility that legal choices will be skewed by the biases inherent in that process. Such biases introduce several risks: that choices will be shaped both by assumptions divorced from sound management and incentives unrelated to public ends; that the rule-bound nature of code will substitute one-time technological “fixes” for ongoing human oversight and assessment; and that the standardization of risk-assessment approaches will eliminate variety—and therefore robustness in risk-management efforts, developing systemic risks of which individual actors may not be aware.

These sorts of systemic effects indicate, at least, that the reluctant-regulator model, characterized by singular reliance on bottom-up commitment by regulated firms for vigorous pursuit of risk-management goals, runs afoul of public-law values regarding the legitimate exercise of regulatory discretion. By this account, resulting decisions may not only be unresponsive to particular goals delegated to the firm, but they may also be literally arbitrary (in that they reflect factors that relevant decisionmakers do not intend to matter), captured by a variety of private concerns, and unaccountable, with significant potential for social harm. As in other regulating-technology contexts, these concerns suggest the need, on the one

315. See Bamberger, supra note 13, at 386–89 (asserting that technology and other complex fields cannot achieve multifaceted goals under traditional rule-based mandates, so experts have increasingly promoted regulation through “incomplete” regulatory instruments that provide greater flexibility and focus on performance instead of concrete rules).

316. See Robert Bartlett, Financial Crises and the Perils of “Safe” Credit 1–3 (Nov. 6, 2009) (unpublished manuscript, on file with author) (discussing the ways in which financial crises frequently arise as a result of a consensus regarding assessments as to which investments are “safe,” the resulting nondiversified investment choices, and the surprising failures in such “safe” markets). See generally John Downer, The Perils of Perfection, RISK & REG., Winter 2009, at 13 (discussing the ways in which aviation technology’s newly developed capacity to standardize aircraft altitude and path accurately has resulted in in-air accidents that were previously statistically impossible).

317. In the words of the Supreme Court, a decisionmaker’s arbitrary—and therefore illegitimate—exercise of delegated discretion is that which “relie[s] on factors which Congress [or agencies] ha[ve] not intended it to consider, entirely fail[s] to consider an important aspect of the problem, offer[s] an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of [decisionmaker] expertise.” See Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983) (observing that the presence of any of these four factors makes a rule of an agency operating under a mandate from Congress arbitrary).
hand, for mechanisms of regulatory-target transparency sufficient to allow meaningful external oversight and expert review even in the presence of proprietary claims over information systems and, on the other hand, for external oversight capacity focused on promoting solid decisionmaking in regulated parties.

B. Proposals for Reform

In light of this catalog of accountability concerns, this subpart explores a different model for envisioning both the function of technology in compliance and the role of the regulator in fostering a more effective capacity to steer private risk management. This model relies on much more intense regulator involvement in oversight and accountability with a threat of sanction. But it also emphasizes collaboration and dynamism in the process of developing risk-management systems, drawing both on private firm information and regulator vantage. Finally, it seeks to better reflect the human decisionmaking element at both levels: the ways human judgment can be skewed by technology, methods for reintroducing that judgment in decision processes, and ways that the limits of both human and computer reasoning might counsel regulatory modesty.

Firms' unchecked development of technology under the umbrella of management-based legal mandates can create independent risk-analysis systems untethered to both legal and long-term management interests. Yet, if information technology possesses a subversive capacity to constitute self-referential and difficult-to-control systems, technology can also offer the unique facility to bridge legal and management systems by making each more visible to the other.

Tapped appropriately, technology's strength can expand regulator capacity to overcome barriers to the observation of firm behavior and can enhance regulators' ability to react to disloyal activities. In short, it can be employed as a mechanism for making firms better regulatory targets. At the same time, more sustained regulator participation in the development of risk-analysis technology can offer regulatory targets greater visibility into regulators' conceptions of meaningful compliance with risk-management mandates, promoting both effective public management, and important rule-of-law and accountability values.

If purely top-down regulatory solutions are ill fitted to risk management and unchanneled bottom-up solutions fall short of public goals, then the third model propounded by certain scholars of new governance offers a starting point for analysis. These scholars, while appreciating the value of process-based regulation, call nonetheless for a more dynamic account of the process regulator as a central standard setter who draws recurrently from "experience at the relatively local level" in order "continually to update the standards all
must meet.” Such an “amended account” is instead “both top-down and bottom-up.”

This dynamic account is especially appealing in the contexts of both risk and technology. While the first frequently involves constant change, the hazards of the second involve ossification of one-time technological fixes where both constant tinkering and paradigmatic innovation may be more appropriate. Yet systems theory predicts that regulated parties will adapt to a static set of external rules with a minimum of change, which, in turn, results only in cosmetic trappings of compliance. A dynamic model of regulation, on the other hand, creates a continuous stimulus that must be translated into meaningful internal practice.

What might this model suggest in the context of technological risk management? And, what advice might it offer policy makers revisiting the administrative institutions and policy approaches that failed to ensure that mandated risk management prevented systemic financial meltdown?

1. Regulatory Target Transparency.—Most basically, the new governance model suggests a fundamental transformation in the legal requirements regarding firm transparency. While disclosure forms a central pillar of risk regulation and technology systems constitute an important tool in compliance with disclosure requirements, transparency as to the decisions made in structuring the systems themselves currently claims little regulatory traction. To be sure, a number of regulatory regimes nod towards the


319. Dorf, supra note 318, at 384.

320. See Kimberly D. Krawiec, Cosmetic Compliance and the Failure of Negotiated Governance, 81 WASH. U. L.Q. 487, 487 (2003) (arguing that these models of regulation “do not deter prohibited conduct within firms and may largely serve a window-dressing function that provides both market legitimacy and reduced legal liability”); see also Bamberger, supra note 13, at 435 (“Once firm decisionmakers know the particular rules for reaching a regulatory safe harbor, and once those approaches have been integrated into corporate understandings of the compliance environment, agency review is likely to exacerbate, rather than ameliorate, pathologies of routinized behavior.”); Kimberly D. Krawiec, Organizational Misconduct: Beyond the Principal-Agent Model, 32 FLA. ST. U. L. REV. 571, 598–99 (2005) (arguing that organizations have perverse incentives to implement ineffective compliance programs).

321. Rubin, supra note 39, at 387; see also id. (“Rather than perceiving the government demand as a single cost, the corporation’s process of self-understanding may lead it . . . to develop a relationship based on genuine compliance.”).
importance of such transparency. Yet they provide neither the granularity nor the frequency of disclosure necessary for either effective or timely analysis.

The Basel II framework, for example, provides an occasion for regulatory transparency by requiring agency preapproval for entities seeking to employ its more flexible, advanced approach to measuring operational risk. The preapproval process requires that regulated entities describe the elements they intend to consider in measuring operational risk. Moreover, the third of the three pillars undergirding the Basel framework is “market discipline through enhanced public disclosures.” Pursuant to this pillar, entities are required quarterly to disclose asset values and capital ratios weighed to reflect market or operational risk, as well as “qualitative” discussions as to “[t]he structure and organization of the relevant risk management function” and “[t]he scope and nature of risk reporting and/or measurement systems.”

The regulations implementing Basel II themselves make clear, however, that banks are provided “with considerable discretion with regard to public disclosure requirements.” Thus, the advanced risk-measurement approaches permitted by the Basel II framework accord financial-services firms significant flexibility in their assessment methodologies and demonstrate no standardized method for measuring, weighing and integrating the methods for assessing risk. They also let bank management “determine[]

---

322. A discussion of regulatory transparency under the Basel II regime follows. See also, e.g., 15 U.S.C. § 7262 (2006) (requiring the annual reports of issuers of registered securities to include statements of responsibility for and assessment of internal control structures and procedures for financial reporting (Sarbanes–Oxley)); id. § 6808 (ordering a study of the information-sharing practices of financial institutions, including the extent and adequacy of their security protections for customers’ personal information (Gramm–Leach–Bliley)); INTERNAL MKT. & SERVS. DG, EUROPEAN COMM’N, ‘SOLVENCY II’: FREQUENTLY ASKED QUESTIONS 7 (2009), available at http://ec.europa.eu/internal market/insurance/docs/solvency/solvency2/faq_en.pdf (requiring insurers to have an “adequate and transparent governance system” and noting that review of governance and risk-management systems will be central to the “supervisory review process” (Solvency II)).

323. BASEL, A REVISED FRAMEWORK, supra note 65, at 148–54.


325. Capital Adequacy Standards for Bank Holding Companies, 12 C.F.R. pt. 225, app. G, § 71 (2009); see also id. § 1 tbl.11.3 (Capital Adequacy) (requiring “[a] summary discussion of the . . . approach to assessing the adequacy of its capital to support current and future activities”); id. § 1 tbl.11.9 (Operational Risk) (requiring a “[d]escription of the [advanced measurement approaches used], including a discussion of relevant internal and external factors considered in the bank holding company’s measurement approach,” and a “description of the use of insurance for the purpose of mitigating operational risk”).


which disclosures are relevant based on a materiality concept,” according “flexibility regarding formatting and the level of granularity of disclosures.” Such discretion is heightened further “if a bank believes that disclosure of specific commercial or financial information would seriously prejudice the position of the bank by making public information that is either proprietary or confidential in nature.” In such circumstances, “the bank need not disclose those specific items, but must disclose more general information about the subject matter of the requirement.”

Not surprisingly, several recent studies of risk-management transparency reveal that “disclosures related to the subject apparently still have a long way to go.” Such disclosures lack the type of detail about the risk-assessment analytics that would permit meaningful assessment of internal controls. These disclosures also lack the sort of standardization that would permit effective comparison of risk across firms. Moreover, the periodic nature of the filings leads to a static, backwards-looking risk focus.

Thus, current regulations fail to capitalize on the very strengths offered by compliance technology. First, the current state of affairs misses the potential for transparency as to the exact methods of quantifying risk and the ways such measures automate decisionmaking. Second, current regulations lack the ongoing capacity to provide timely and evolving risk information.

Remedying this failure to provide the granularity necessary for effective analysis would require several moves. First, regimes need to be introduced to standardize reporting on risk-management technology, as well as successes and failures, so that regulators can assess the promise and outcomes of different risk approaches on the ground and compare them.

Opinions, in OPERATIONAL RISK TOWARD BASEL III: BEST PRACTICES AND ISSUES IN MODELING, MANAGEMENT, AND REGULATION 3, 4 (Greg N. Gregoriou ed., 2009). Nevertheless, the Basel II framework leaves discretion as to how to combine them, and there are neither formal, nor generally accepted, methodologies for their reporting. Guy Ford et al., Operational Risk Disclosure in Financial Services Firms, in OPERATIONAL RISK TOWARD BASEL III: BEST PRACTICES AND ISSUES IN MODELING, MANAGEMENT, AND REGULATION, supra, at 381, 384.


329. Id.

330. Id. The SEC’s Regulation S-K thus requires disclosure of only “description[s]” of underlying financial models used in assessing periodic financial filings. See, e.g., 17 C.F.R. § 229.305(a)(ii)(B) (2009) (providing that “[r]egistrants shall provide a description of the model, assumptions, and parameters”); id. § 229.305(a)(iii)(B)(1)(i) (requiring provision of “[t]he average, high and low amounts, or the distribution of the value at risk amounts for the reporting period”).

Standardized requirements would mandate the detailed submission of the code and operational specifics of compliance-technology systems as well as results of the regular testing and monitoring of control effectiveness that the technology enables. Such broad-based measures could draw on agency-specific efforts such as those of the FDA, which already requires pharmaceutical companies to submit confidential, trade-secret, and private information, such as ongoing test data on drug safety and effectiveness.332 Alternatively, regulators might insist on more targeted submissions, such as those required by the Federal Reserve Bank for stress testing of certain large banks in the wake of the financial crisis.333 Requiring such granularity in reporting can promote transparency to regulators and to firm managers, who themselves may not possess full familiarity with the choices embedded by third-party technologists responsible for systems’ development and implementation.

Regimes promoting such reporting might further require incorporation of a variety of policy mechanisms to incentivize disclosure on the part of interested parties. Regulated firms themselves might be compelled to reveal technology systems developed internally under direct pressure from the regulators to whom they answer. Yet to prompt disclosure from third-party vendors (over whom individual agencies would likely have no jurisdiction), regulators might employ additional measures, such as the development of certification systems.334

Moreover, the ability to combine standardized approaches with enhanced public disclosure of certain elements of risk information can enlist robust input and oversight by third parties including investors, analysts, academics, and nonprofits.335 This approach has been taken in the SEC’s recent moves towards requiring public companies and mutual funds to use the interactive eXtensible Business Reporting Language (XBRL) format for data contained in filings with the agency.336 And while confidentiality and

332. See, e.g., Financial Disclosure by Clinical Investigators, 21 C.F.R. § 54 (2009) (requiring disclosure of financial interests of clinical investigators in the success or failure of the drugs they are testing).


334. For further explanation of policy mechanisms for promoting disclosure of computer code in the context of voting technology, see generally Hall, supra note 309.

335. Erik Gerding in fact argues that such technology should be fully open source. Gerding, supra note 241, at 179.

proprietary concerns need to be considered, moves by the FDA, for one, have taken an important lead in suggesting that, where public risks are involved, the balance has tilted too far in the direction of secrecy. In its recent establishment of a “Transparency Task Force,” the FDA has embraced the goal of making “useful and understandable information . . . available to the public in a timely and user-friendly format”\(^3\)\(^3\)\(^7\)--a goal that can leverage private regulatory oversight considerably.

2. Regulator Reform.—Transparency into the workings of regulated firms, however, provides only half the prescription. A new governance model further requires significant investment in the competence of administrative agencies themselves—both in terms of technical expertise and computing capacity.\(^3\)\(^3\)\(^8\) Regulators constrained by limited resources cannot currently keep up with the massive data-processing capacity of private corporations.\(^3\)\(^3\)\(^9\) Many have not developed the necessary staff capacity for robust analysis of the various analytic approaches employed by such firms.\(^3\)\(^4\)\(^0\) And, even when agency staff claim technical expertise, institutional structures may not be geared to promote the independent analyses of technological approaches necessary to probe meaningfully into the static, institutionalized assumptions underlying accepted risk-management practices.\(^3\)\(^4\)\(^1\) Indeed, especially where an agency draws its technologically sophisticated staff from a pool that shares training and experience with those responsible for technological development and implementation within private firms, regulator analyses produce similar analytical failures.

---


\(^3\)\(^3\)\(^8\). See generally ANELISE RILES, Placeholders: Engaging the Hayekian Critique of Financial Regulation, in COLLATERAL KNOWLEDGE: LEGAL REASONING IN THE GLOBAL FINANCIAL MARKETS ch. 5 (forthcoming 2010), available at http://ssrn.com/abstract=1492065 (discussing the truth of Friedrich Hayek’s insight that public expertise, or bureaucratic knowledge, is inherently one step behind the market, preventing effective market planning, but arguing on the other hand that the flaws of private decisionmaking justify enhancing regulatory capacity nonetheless).

\(^3\)\(^3\)\(^9\). See O’Harrow & Gerth, supra note 292 (detailing how, because of limited resources, N.Y. Federal Reserve Chief Tim Geithner was entirely reliant on the assessments of big banks about their activities).

\(^3\)\(^4\)\(^0\). See, e.g., Elizabeth A. Nowicki, 10(b) or Not 10(b)?: Yanking the Security Blanket for Attorneys in Securities Litigation, 2004 COLUM. BUS. L. REV. 637, 710–11 (describing how chronic understaffing at the SEC limits its enforcement abilities); Jay W. Verret, Dr. Jones and the Raiders of Lost Capital: Hedge Fund Regulation, Part II, a Self-Regulation Proposal, 32 DEL. J. CORP. L. 799, 817 (2007) (illustrating why hedge-fund regulators trail private actors in technical competence regarding new financial products).

\(^3\)\(^4\)\(^1\). See, e.g., Nowicki, supra note 340, at 709–11 (asserting that pressures on the SEC prevent effective regulation because SEC lawyers are hesitant to regulate their peers and upset the private bar); O’Harrow & Gerth, supra note 292 (explaining that bank regulators at the Federal Reserve Bank of New York may have been too closely tied to private financial institutions to effectively oversee and enforce risk-management regulations against those institutions).
Therefore, administrative structures and processes geared towards ameliorating “cognitive” independence, capture, and turf problems must be part of any restructuring by financial regulators, especially in the development of systemic risk-regulation capacity. These structures might be drawn from successful experiments in other contexts such as the Department of Homeland Security’s (DHS) Data Privacy and Integrity Advisory Committee (DPIAC)—an external oversight body comprised of privacy and security experts from the public and private sectors with sophisticated knowledge of both technology and privacy—which analyzes DHS’s technology choices before they are made.\(^{342}\) Additionally, in an attempt to pierce the opacity of risk-management-technology choices, these administrative structures can provide the strength of peer review from a variety of viewpoints as well as insight into the type of situation faced by financial regulators who ultimately had to rely on intuition about the strength of private-party risk management.\(^{343}\)

3. **Dynamic Activist Regulation.**—Armed with greater expertise and information, regulators can engage in more robust, albeit collaborative, participation in the ongoing development of effective risk management. This can occur in a number of ways consistent with the regulatory vision of developing “rolling best practices” by collecting data from regulated entities (about what works and what does not) and disseminating that information back, through education and capacity building.\(^{344}\) It can also permit regulators a greater sense of whether firms are committed to effective and dynamic risk-regulation efforts or are simply engaged in cosmetic compliance efforts in a way that masks skewed incentive systems and unreasonably risky activities or even tends to outright fraud and misrepresentation. It thus enables regulatory enforcement and sanctioning as means of spurring compliance.\(^{345}\)


\(^{343}\) See O’Harrow & Gerth, supra note 292 (relaying that a confidential review by N.Y. Federal Reserve Bank discovered that “banking companies could not properly assess their exposure to a severe economic downturn and were relying on the ‘intuition’ of banking executives rather than hard quantitative analysis”).

\(^{344}\) Dorf & Sabel, supra note 318, at 350.

\(^{345}\) See Bamberger, supra note 13, at 465 (pointing to the regulatory model-settlement agreements, which “are characterized not just by cooperation, but by cooperation ‘in the shadow’ of enforcement”).
a. Increasing Guidance.—First, while financial regulators have, to date, taken a hands-off approach regarding specific technologies and approaches, administrative agencies in other contexts have pioneered practices to improve compliance guidance. The FDA has, for example, initiated informal meetings with technology providers in an attempt to learn about the capacity of technology products geared towards managing risks of the drug-approval and testing process. The FTC has gone further, having established a program of workshops aimed at firms and GRC developers on how best to comply with privacy regulations. At these workshops, the agency brought together developers of a number of systems, including Oracle, IBM, and AT&T Labs, to address questions on compliance. The FTC then made the transcripts of the 2003 workshop panels available through their website and has also made videotapes of the sessions available.

b. Enhancing the Ex Ante Approval Lever.—Second, financial regulators might, again taking cues from the FDA, engage in forms of “approval regulation” by which individual financial institutions or technology providers would provide full transparency regarding proposed risk-management technologies ex ante and agree to greater disclosure in exchange for a form of legal safe harbor or “certification” in implementation. Such an iterative process of disclosure and approval could easily be incorporated into the Basel II framework, for example, by hinging approval to engage in the regime’s advanced risk-management techniques on the requisite transparency and engagement. Such approvals, moreover, could be done in a limited or experimentalist manner, permitting the gathering of outcomes, data, and information that would further inform the best-practice evolution.

c. Reintroducing Human Judgment.—Third, a robust and informed focus on risk-management practices on the ground, moreover, might permit regulators to direct firms away from overreliance on technology exclusively and towards the reintegration of human judgment, from which management-

346. See Stephen A. Raymond & Gerald F. Meyer, Interpretation of Regulatory Requirements by Technology Providers, 11 APPLIED CLINICAL TRIALS 50, 50-51 (2002) (noting that with the help of clinical-trial sponsors and technology providers, the FDA developed regulations to facilitate the use of computer systems and data-processing technology in the submission of clinical trials).


349. See Fed. Trade Comm’n, supra note 347.

based regulation was originally intended to draw. It is increasingly clear from the evidence that risk-management success depends in large part on the extent to which technology is used to support decisions as well as automate them. Goldman Sachs's relative risk-management success rests both on the fact that their technology flagged anomalous loss trends and on the response to those flags: Goldman's culture promoted immediate up-the-line reporting, which permitted a firm-wide shift in investment strategy and the resulting business rules governing individual traders' actions.

The role of human judgment in internal decision processes has been strengthened by regulation in other contexts, notably Sarbanes–Oxley, which focused not only on "enhancing disclosure," but also on "altering incentives to change behavior." Specifically, Sarbanes–Oxley's certification requirements provide for what might be called "attention regulation" by placing responsibility for thinking about control systems on particular officers, who must articulate the reasoning behind choices made in structuring programs and attest to their adequacy in public documents. This model has—by identifying specific individuals that must assess and focus on particular risk-management elements—been credited with making "senior executives in a company take their financial reporting seriously," and it might be employed by forcing other individuals to focus attention on specific red flags through reporting requirements and explanation to administrative bodies.

Research in socio-technical studies suggest the promise of similar approaches in regulating the role of technology in risk decisionmaking. Robust disclosure regarding risk-management systems must include not only technical specifications, but also information regarding the ways in which technical systems involve human beings: how those systems are developed, how the decisions they embed are overseen, in what ways their outputs prompt or automate decisions, and how those decisions are reviewed by humans. Individual human beings within firm decision structures, moreover, can be mandated by regulation to review technological decisions, to certify and take responsibility for them, and to explain the decisions to regulators and other outside parties—in short, to exercise the judgment delegated to them. Such requirements should be triggered by periodic requirements,

---


352. Bamberger, supra note 13, at 385.


354. See, e.g., Murray G. Millar & Abraham Tesser, Thought-Induced Attitude Change: The Effects of Schema Structure and Commitment, 51 J. PERSONALITY & SOC. PSYCHOL. 259, 269 (1986) (suggesting that the complexity of cognitive schema—together with the existence or nonexistence of a prior commitment to a particular attitude toward an object—determine the subsequent polarization of attitudes toward that object); Angelo C. Valenti & Abraham Tesser, On
but also by individual occurrences such as loss events or systemic trends. These processes, and the resulting decision feedback, have, in a variety of contexts in which humans and computer systems interact, increased social accountability of decisionmakers. The resulting choices arise from an open-loop or learning approach that takes account of a variety of viewpoints, rather than a closed-loop, automated process. This, in turn, reduces instances of automation bias through decreased errors of omission and commission and improves overall task performance. By these means, technology can better be cabin'd to the role of decision support, rather than decisionmaker.

d. Regulatory Precaution.—Finally, and very differently, greater familiarity with and participation in risk-management capacity in action might promote greater regulator realism as to the feasibility of risk management. This realism, in turn, might profoundly change default assumptions in policy making, as well as particular policy choices. Regulators who are acutely aware of technological limitations on the ability to develop real-time analysis and to analytically assess uncertainty may have a more difficult time ignoring the fact that unforeseen failures will occur with relative certainty. This might have deep implications for choices such as whether to allow firms to trade in new and uncertain financial products or at what level to set capital reserves so that losses can be contained, and it suggests a new approach towards precaution in regulation.
VI. Conclusion

The burgeoning role of technology in the implementation of legal mandates focuses longstanding governance debates through a twenty-first-century prism. Sources of contemporary risk—from financial, to operational, to informational risk—are characterized by the heightened scope, speed, and interdependence of human transactions, behaviors, and the technologies that enable them. Informational asymmetries between private fora in which risk originates and the public actors who regulate them are intensified. And those charged with making decisions about managing risk—whether administrative agencies or those they regulate—must increasingly turn to technological methods of prediction and decision to carry out the risk-management processes with which they are tasked.

Yet, as in any context in which human judgment must rely on scientific, quantitative, and analytic inputs, decision systems can create secondary risks that impede the sound exercise of discretion. Such systems are necessary in analyzing complicated manifestations of risk. Yet their apparent sophistication, neutrality, and precision mask an incapacity to reflect uncertainty, the opacity of the values they embody, and the consequent ways in which they disable the reasoned judgment of the human decisionmakers they inform.359

Faced with this reality, a reticent approach to regulation cannot square with important principles of good governance. Those delegated regulatory discretion by our public-law system must be held accountable by others, both in the public and in the private sector. Such oversight—rather than mistake, bias, or self-interest—must guide decisions about the appropriate measures that must be taken to reduce the social cost of risk. Human judgment must be integrated rather than forced out, reflecting the reality that “better prediction products arise more from the feedback between predictions and experience than from the introduction of more sophisticated predictive methodologies.”360 And policy makers must let the fact of imprecision—human and technical—govern their decisions, recognizing the need to guard against disaster in the face of uncertainty. Anything less would be an abdication of regulatory responsibility.

