

TECHNOLOGIES OF COMPLIANCE:
RISK AND REGULATION IN A DIGITAL AGE

KENNETH A. BAMBERGER

ABSTRACT

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 \$60 billion last year, and this growth is poised to increase exponentially.

While these technology systems offer powerful compliance tools, they also court danger. They permit computer programmers to interpret legal requirements; they mask the uncertainty of the very hazards with which policymakers 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, and proposes specific reform measures for policymakers revisiting the governance of systemic risk. While regulators have lauded the turn to technology, they have ignored its perils. 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.

TECHNOLOGIES OF COMPLIANCE:
RISK AND REGULATION IN A DIGITAL AGE

TABLE OF CONTENTS

INTRODUCTION	1
I. NEW GOVERNANCE AND THE PROCEDURAL REGULATION OF RISK.....	7
II. THE TURN TO TECHNOLOGY, AND ITS BENEFITS	12
A. TECHNOLOGY’S EFFICIENCIES	13
B. TECHNOLOGY’S EFFECTIVENESS	14
1. <i>The IT Toolbox</i>	14
2. <i>“Governance, Risk and Compliance” Systems</i>	16
III. TECHNOLOGY PITFALLS AND THE CHALLENGE FOR GOVERNANCE	29
A. THE RETICENT REGULATOR	30
B. THE PERILS OF TECHNOLOGY	33
1. <i>Problems of Translation</i>	33
2. <i>Systemic Effects</i>	37
3. <i>Cognitive Bias in Decisionmaking</i>	38
4. <i>Technology Failures and the Financial Crisis</i>	41
C. GOVERNANCE IMPLICATIONS	46
IV. PROPOSALS FOR REFORM.....	48
A. REGULATORY TARGET TRANSPARENCY.....	50
B. REGULATOR REFORM	53
C. DYNAMIC ACTIVIST REGULATION	54
1. <i>Increasing Guidance</i>	55
2. <i>Enhancing the Ex Ante Approval Lever</i>	55
3. <i>Reintroducing Human Judgment</i>	55
4. <i>Regulatory Precaution</i>	57
CONCLUSION.....	58

TECHNOLOGIES OF COMPLIANCE:
RISK AND REGULATION IN A DIGITAL AGE

KENNETH A. BAMBERGER *

INTRODUCTION

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 both by selling some of its mortgage-backed securities, and by diversifying its holdings to hedge the risk of others.¹ While Goldman suffered losses in 2007, they reached nowhere near the scale of those suffered by its contemporaries.² The firm avoided the fate of now-defunct competitors

© 2009, Kenneth A. Bamberger.

*Assistant Professor of Law, University of California, Berkeley, School of Law. This project was supported in part by funding from the Berkeley Center for Law and Technology (BCLT), and from TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422).

I am very appreciative for thoughtful insight from Miriam Bitton, Danielle Citron, Larry Cunningham, Dan Farber, Cristie Ford, Yuval Feldman, Erik Gerding, Bob Glushko, Kimberly Krawiec, Doug Kysar, Christine Parker, Oren Perez, Jeff Rachlinski, Pam Samuelson, AnnaLee Saxenian, William Simon, Susan Sturm, Tom Tyler, Molly Van Houweling, Cynthia Williams, Stepan Wood, David Zaring, and other participants at the University of British Columbia/Canada Social Sciences and Humanities Research Council's 2009 Conference on "New Governance and the Business Organization;" the Israel Science Foundation/Bar Ilan University 2009 Conference on "The Regulatory State at the 21st Century;" and faculty roundtables at the UC Berkeley Law School, the UC Berkeley School of Information, and the BerkeleyLaw Junior Working Ideas Group (JWIG).

Aaron Brauer-Rieke, Tim Byron, and Sumeet Ajmani provided exceptional research assistance.

¹ Joe Nocera, *Risk Mismanagement*, N.Y. TIMES, Jan. 4, 2009

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 Heard on The Street: Goldman's Price of Protection*, WALL ST. J., March 18, 2009, at C4 ("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.").

Bear Stearns and Lehman Brothers; it is projected to earn record profits in 2009.³

The meeting's fortuitous timing was no coincidence. Since the 1980s, Goldman had invested heavily in risk-modeling technology.⁴ Unlike some of its competitors, Goldman's system had incorporated into its monitoring capacity daily trend reporting, based on sophisticated quantitative risk-prediction programs.⁵ In December 2006, Goldman's system indicated a problem—the firm's daily profit and loss reports showed that its mortgage business had posted a loss for ten straight days.⁶ 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 systems, software and analytics—in assessing and controlling risk, and in compliance 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, including 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.⁷ This “process-based” or “management-based” model⁸ responds to the combination of

³ Christine Harper, *Goldman Sachs Reverts to Pre-Lehman Risk Mean as Profits Surge*, Bloomberg.com, July 10, 2009, available at <http://www.bloomberg.com/apps/news?pid=20601103&sid=axo2pKtI0rts>

⁴ *On Top of the World: Goldman Sachs*, ECONOMIST, Apr. 29, 2006.

⁵ Nina Mehta, *One on One Interview With Emanuel Derman*, Financial Engineering News, July/Aug. 2003 (in which former Goldman Sachs risk modeler Emanuel Derman said, “In a good way, Goldman Sachs was eclectically irreligious 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.”) (available at <http://www.ederman.com/new/docs/fen-interview.html>).

⁶ Nocera, *supra* note __.

⁷ See Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L. J. 377 (2006) (describing the model).

⁸ Cary Coglianese & David Lazer, *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals*, 37 L. & SOC. REV. 691 (2003),

challenges that often make risk regulation difficult. Risk is contextual, and manifests itself differently across heterogeneous firms. Regulated firms have far better information the agencies that oversee them about firm organization, and about the sources of risk and capacity for risk mitigation. 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 the type of uniform rules setting particular measurable outcomes prevalent in much environmental regulation.

Much modern risk regulation, therefore, takes a different tack, eschewing mandated outcomes and requiring instead that regulated firms develop individualized internal risk-management *processes*. Such regulation identifies risk-mitigation goals generally—such as “managing the risks associated with” the over-the-counter derivatives trade.⁹ 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, then, implementation by private institutions ultimately animates the law’s meaning.

In response to such requirements, regulated firms have turned to technology. Given the scale and complexity of contemporary business institutions, and the massive amount of information involved in corporate operations, the types of risk controls for which government mandates call simply cannot function without the data collection, analytic and monitoring capacities of integrated computer technology. Government regulators thus urge compliance through “increasing standardization and automation,”¹⁰ and the use of “forensic tests and new technology.”¹¹ Third party software vendors offer “fully-automated risk analytics and controls.” Influential consulting firms and auditors further contribute: IBM promotes a “Unified Governance Framework” based on

⁹ See 17 C.F.R. § 240.15c3-4(a) (2006) (“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.”).

¹⁰ Roger T. Cole, Director, Division of Banking Supervision and Regulation, Federal Reserve Bank, *Risk Management in the Banking Industry*, Testimony Before the Subcommittee on Securities, Insurance, and Investment, Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Washington, D.C., March 18, 2009.

¹¹ Lori A. Richards Director, Office of Compliance Inspections and Examinations U.S. Securities and Exchange Commission, *Compliance in Today's Environment: Step Up to the Challenge, Remarks Before the LA Compliance Best Practices Summit 2009 of the Investment Adviser Association*, Washington, D.C., March 12, 2009.

extensive software research into REALM (REgulations As Logical Models); Deloitte studies document the economies gained by automating risk management controls; while one Ernst and Young partner concludes simply: “The more controls a company can move from manual to automated, the better.”¹²

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 \$60 billion last year. 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.¹³

GRC systems, indeed, offer powerful compliance tools. They typically automate the integration and analysis of huge amounts of data, inform high-level decisionmakers accordingly regarding levels and locations of risk, and “force” consequent 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,¹⁴ 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

¹² Sharyn Kohen, *New Tech Boosts Compliance Tests*, BANK TECH. NEWS 49 (Oct. 2005).

¹³ Binyamin Appelbaum and David Cho, *Geithner to Propose Vast Expansion Of U.S. Oversight of Financial System*, WASH. POST, March 26, 2009; at A01 (“The Obama administration’s plan, described by several sources, would extend federal regulation for the first time to all trading in financial derivatives and to companies including large hedge funds and major insurers such as American International Group. The administration also will seek to impose uniform standards on all large financial firms, including banks, an unprecedented step that would place significant limits on the scope and risk of their activities.”)

¹⁴ Below, at Part III.B.3.

speculation, and intentional manipulation, with a façade of regularity. In the words of former Federal Reserve Chairman Alan Greenspan, the “whole 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.”¹⁵

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 private firms broad authority to develop their own risk-management controls allows those firms to fill out the meaning of legal norms, 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.”¹⁶

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 as to how the law is interpreted. Those choices may be shaped by a variety of extra legal 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.¹⁷ While technology-based compliance systems have proliferated specifically in contexts in which legislators and policymakers have rejected rule-based mandates in favor of context-specific judgment by regulated entities, computer code operates by means of on-off rules, while the analytics it employs seek “to quantify the immeasurable with great precision.”¹⁸

¹⁵ House Committee on Oversight and Government Reform, Hearing of October 24, 2008 (testimony of Alan Greenspan).

¹⁶ Joel R. Reidenberg, *Lex Informatica: the Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); LAWRENCE LESSIG, *CODE, VERSION 2.0*, p.1 (2006) (“Code is Law.”).

¹⁷ H. Itami & T. Numagami, *Dynamic Interaction Between Strategy and Technology*. 13 STRATEGIC MANAGEMENT J. 119 (1992).

¹⁸ Nassim Taleb, *Against Value-at-Risk: Nassim Taleb Replies to Philippe Jorion* (1997), available at <http://www.fooledbyrandomness.com/jorion.html>.

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 policymakers are concerned, and clouding the judgment of users on which 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 phenomena are at the heart of the failure of risk regulation, and risk management, to prevent the current financial meltdown.

For these reasons and others, moreover, 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 their development 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 regarding the exercise of regulatory discretion.

This paper proceeds by exploring these phenomena, and the failure of risk regulation to address them. Parts I and II describe prevailing "management-based" or "process-based" approaches to financial and operational risk regulation, and the inevitable push towards technology systems as a means for compliance with legal and managerial requirements for risk management.

Part III in turn describes the "perils" of technological compliance—the ways in which technology systems intended to manage risk themselves can both mask both uncertainty and malfeasance, and create 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.

Finally, Part IV proposes specific regulatory reforms for policymakers revisiting the regulation of both firm-wide and systemic risk. 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 capable of market oversight with significantly enhanced access to the workings of organizational decisionmaking, and thus provide 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 both effective policy and important rule-of-law and accountability values.

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 the broader vantage of the administrative agency. Perhaps most importantly, it seeks better to 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.

I. NEW GOVERNANCE AND THE PROCEDURAL REGULATION OF RISK

The risks generated by individual firm operations create significant social costs. The inaccurate assessment of the risks that occur as a result of existing as a business, or risk taken on with the purpose of calculated reward, like market or capital risk, can externalize significant costs on consumers, investors, and other market players. The failure to address synthetically the ways in which the risk of any individual enterprise is interdependent with industry risk generally, moreover, 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, business focus, and operational procedures within individual firms are heterogenous. Thus 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,¹⁹ much of the damage is irreversible. Such *ex post* legal measures can do little to either undo much of the resulting social harm, or provide requisite restitution—not least of which because many of the targeted institutions have ceased to exist.

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 trying to prescribe behavior that will lead to particular outcomes in a system (business or economics) governed by a different, or even incommensurate, rationality.²⁰ This account, in turn, suggests a “new” approach to governance.²¹ 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 those decisions’ outcomes.

Consistent with these insights, regulatory efforts at curbing risk itself have largely focused instead on regulating risk *management*. Such “management-based” or “process-based” regulation²² articulates public goals, and requires regulated firms to develop internal processes and controls geared towards their achievement. Yet it delegates to regulated

¹⁹ See e.g., lawyerlinks.com, at http://content.lawyerlinks.com/default.htm#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”).

²⁰ Niklas Luhmann, *The Unity of the Legal System*, in Gunther Teubner ed., 12 *AUTOPOIETIC LAW: A NEW APPROACH TO LAW AND SOCIETY* (1987). For an account that emphasizes the demise of state-centered regulation, see Philip G. Cerny, *Embedding Global Financial Markets*, in PRIVATE ORGANIZATIONS IN GLOBAL POLITICS 59 (Karsten Ronit & Volker Schneider eds., 2000).

²¹ See Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 *MINN. L. REV.* 342 (2005) (describing this body of scholarship).

²² See generally Coglianesse & Lazer, *Management-Based Regulation*, *supra* note ___, at 696–700 (describing the use of management-based regulation in the areas of food safety, industrial safety, and pollution prevention).

entities themselves wide discretion in deciding how to interpret and achieve those goals in particular context. Such “regulatory delegation” thus enlists the judgment of firm decisionmakers to draw on superior knowledge of internal firm workings inaccessible to regulators, and seeks to harness firm risk-management systems as regulatory assets by aligning public and private incentives.²³

This approach dominates the regulation of financial institutions. Regulation governing the “safety and soundness” of banks, for example, relies largely on process. 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,” which provide for: effective risk management; adequate safeguards for asset management; legal compliance; structures and systems geared to internal monitoring and audit; and accurate reporting.²⁴ Moreover, banks must “maintain a system” to identify problem assets and prevent their deterioration, involving 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.”²⁵

The “Basel II” banking regulation regime similarly relies on internal processes to derive bank capital adequacy requirements in light of credit, operational, and market risk.²⁶ Specifically, the international accord permits national regulators to allow large institutions to opt out of standard capital requirements if they use internal risk models that meet certain standards. 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,²⁷

²³ Ian Ayres & John Braithwaite, *RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE* (1992).

²⁴ *Interagency Guidelines Establishing Standards for Safety and Soundness*, 12 C.F.R. Part 364, Appendix A, § II.A. (developed by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision).

²⁵ *Id.* at § II.G.

²⁶ The international Basel II Accord embodied recommendations on banking regulation developed by the central bank Governors of the Group of Ten nations through the Basel Committee on Banking Supervision,

²⁷ 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 outlining the implementation of Basel II, for example states 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

but ultimately “the 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.”²⁸

Other regimes governing financial institutions require banks to establish “internal controls” furthering compliance with the U.S. Patriot Act, the Bank Secrecy Act and other anti-money laundering requirements.²⁹ They require investment advisors to adopt policies and procedures “reasonably designed to ensure that [the adviser] vote[s] . . . in the best interest of clients.”³⁰ And they require derivatives dealers to “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.”³¹

More broadly, firms in a variety of sectors that possess different types of personally-identifiable financial and health information must establish “risk assessment and data security systems”³² to protect its

in less liquid markets, and determine the effect that these exposures might have on capital adequacy. 12 C.F.R. 3, 208, 225, 325, 567 (2007), available online at <http://www.occ.gov/ftp/release/2008-81a.pdf>. Similarly, any determination of market risk should consider, “factors such as illiquidity of instruments, leverage, concentrated positions, one-way markets, non-linear 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.* at 12.

²⁸*An Update on Basel II Implementation in the United States* (Feb. 26, 2007) (Speech by Fed Governor Susan Schmidt Bies to the Global Association of Risk Professionals Basel II Summit), available at <http://www.federalreserve.gov/newsevents/speech/bies20070226a.htm>.

²⁹ Bank Secrecy Act/Anti-Money Laundering Examination Manual, available at <http://www.occ.treas.gov/handbook/BSA-AMLexamprocedures.pdf>

³⁰Investment Advisers Act Rule, 17 C.F.R. § 275.206(4)–6(a) (2006).

³¹ See 17 C.F.R. § 240.15c3-4(a) (2006) (“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.”).

³² Title V of the Gramm-Leach-Bliley Act (GLB), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–6827 (2000)) empowers various agencies to promulgate data security regulations for financial institutions. 15 U.S.C. §§ 6801, 6805. The Federal Trade Commission’s 2003 standard implementing the Act in turn 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

privacy and security. And under Section 404 of the Sarbanes Oxley Act, perhaps the most notable example of a management-based regulatory regime, *all* publicly-traded companies must develop internal controls for assuring the accuracy of financial reports and disclosures. The administrative guidance implementing Sarbanes Oxley requires evaluation of various elements of internal controls; yet it leaves firm management wide discretion in its assessment approach.³³

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 expansion of risk-management oversight in previously unregulated contexts. 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.³⁴ 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.³⁵

information at issue." 16 C.F.R. § 314.3 (2006). 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 particular implementation is left to individual firms, and "[t]he ultimate test remains a broad one, that of 'reasonable data security.'" Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. (2007) (quoting Interagency Guidelines Establishing Information Security Standards, 69 Fed. Reg. 77,620 (Dec. 28, 2004)).

³³ See Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5, and the SEC's interpretive guidance. Procedure-based mandates, moreover, arise from a combination of public and private sources. The enterprise risk management framework developed by the private-sector Committee for Sponsoring Organizations of the Treadway Commission (COSO), see Committee of Sponsoring Organizations of the Treadway Commission, ENTERPRISE RISK MANAGEMENT - INTEGRATED FRAMEWORK (2004), 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—including appropriate risk assessment, institutional risk responses, and control activities; yet it 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 Listing Standards*, Part 7d.

³⁴ See *Request For Comment: Enterprise Risk Management Analysis For Credit Ratings Of Nonfinancial Companies*, available at <http://www2.standardandpoors.com/spf/pdf/fixedincome/615344ERM%20Analysis.pdf>.

³⁵ See generally European Commission, *Solvency*, available at http://ec.europa.eu/internal_market/insurance/solvency/index_en.htm. The Solvency

Although these initiatives address a variety of substantive ills, they share certain important governance characteristics. Much as Congress sets forth broad statutory aims and frameworks but delegates to administrative agencies the task of filling in the substantive detail, these regimes similarly articulate general goals, yet largely delegate to regulated firms themselves the decisions about specifics: everything from the meaning of the public aim in particular context (identifying and mitigating a variety of risks, preventing financial fraud or misrepresentation, protecting sensitive information) to the means for achieving it. Certainly, some regulatory delegations (as with some statutory delegations) offer more precision than others, specifically requiring that regulated firms employ general management processes, or 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. To this extent, private firms are made partners in regulation, implicitly and explicitly enlisted to fill out the substance of public legal norms.

II. 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 complexity of compliance burdens, or 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

II regime has been called a “Basel for Insurance,” see KPMG, *Study Into The Methodologies to Assess the Overall Financial Position of an Insurance Undertaking from the Perspective of Prudential Supervision* (May 2002), available at <http://intranet.icea.es/solvencia/Documentos/KPMG%20solv%20final%20report-300402.pdf>

effectiveness—the trend towards embedding risk management in technology systems is inevitable.³⁶

A. Technology's Efficiencies

The cost of compliance with management-based risk regulations has been staggering. At least one study has estimated that the start-up costs in the implementation of Sarbanes-Oxley's requirements alone have cost U.S. businesses \$1.4 trillion.³⁷ 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.³⁸

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

First, the greatest source of the increase in compliance spending has arisen from compensation of staff responsible for manual oversight of compliance controls.³⁹ 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.⁴⁰ 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.”⁴¹

³⁶ See, e.g., Ernst & Young, CORPORATE REGULATORY COMPLIANCE PRACTICES (2005) (documenting the number of companies that use technology to track compliance and management, monitor compliance controls, and handle regulatory reporting).

³⁷ Ivy Xiyang Zhang, *Economic Consequences of the Sarbanes-Oxley Act of 2002* (2002), available at http://w4.stern.nyu.edu/accounting/docs/speaker_papers/spring2005/Zhang_Ivy_Economic_Consequences_of_S_O.pdf.

³⁸ Deloitte Center for Banking Solutions, *Navigating the Compliance Labyrinth* (Jan 2008).

³⁹ *Id.*

⁴⁰ See MICHAEL G. SILVERMAN, COMPLIANCE MANAGEMENT FOR PUBLIC, PRIVATE, OR NONPROFIT ORGANIZATIONS 203 (2008).

⁴¹ See *id.* at 212.

Finally, automation has permitted the alignment of the compliance function with business operations. Compliance has traditionally been managed separately from the risk management function exercised by operational managers. 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 the large modern corporation who must each be trained in complicated organizational business and compliance rules, leaves openings for inconsistency, mistake, or outright fraud.⁴² Employee incentive systems complicate the balance of performance metrics with those measuring risk.⁴³ Manual oversight and controls testing must typically be limited to spot-checks because of workload constraints. And systemic analysis of the flood of information that results, especially in data-intensive industries, is often impossible. The variety of data management and analysis tools available through modern information technology systems offers firms' a means to address each of these shortcomings.

1. *The IT Toolbox*

The power of information technology systems arise from their ability to manage, organize and analyze massive amounts of data with uniformity and particularity, and then structure decisionmaking accordingly.

Most simply, computer systems permit the creation of a consistent identification scheme for digital information across all

⁴² See generally 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) ("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.")

⁴³ See *The Growing Importance Of Enterprise Risk Management*, Forrester Research Blog For Information & Knowledge Management Professionals (post of Research Director Kyle McNabb) available at http://blogs.forrester.com/information_management/2009/01/the-growing-imp.html.

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—in every relevant business process. Software code is rule-based in nature, and automated decision-making software tends to be formed primarily of declarative logical statements, which can be combined into decision-tree-like branches.⁴⁴ 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.”⁴⁵

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.”⁴⁶ Analytic models, which 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.⁴⁷

⁴⁴ See JAMES TAYLOR, SMART (ENOUGH) SYSTEMS: HOW TO DELIVER COMPETITIVE ADVANTAGE BY AUTOMATING HIDDEN DECISIONS 150 (2007)

⁴⁵ James Grimmelman, *Regulation by Software*, 114 YALE L.J. 1719, 1734 (2005).

⁴⁶ THOMAS H. DAVENPORT & JEANNE G. HARRIS, COMPETING ON ANALYTICS: THE NEW SCIENCE OF WINNING 7 (2007).

⁴⁷ ANTHONY TARANTINO, THE GOVERNANCE, RISK, AND COMPLIANCE HANDBOOK: TECHNOLOGY, FINANCE, ENVIRONMENTAL, AND INTERNATIONAL GUIDANCE AND BEST PRACTICES 217 (describing how these risk analysis techniques

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.”⁴⁸ Such “business intelligence” software thus can both “analyze, forecast, predict, optimize” but also “collect[], manag[e], and report[] decision-oriented data.”⁴⁹ These functions are essential for compliance not only for procedural risk-management mandates, but also with regulatory reporting requirements, such as Sarbanes Oxley’s requirement that users of corporate data “demonstrate that their decisions are based on trustworthy, meaningful, authoritative, and accurate data.”⁵⁰

2. “Governance, Risk and Compliance” 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.

The products and systems available in the market differ in scope and offerings. Industry leaders such as Axentis, BWISE, IBM, OpenPages, Oracle, SAP and Paisley⁵¹ provide comprehensive compliance and risk management platforms with packages geared towards a variety of more common regulatory regimes such as Basel II, SoX, and privacy and fraud laws; SAP’s compliance solutions even include offerings targeted to compliance with the Clean Air Act⁵² and the Bioterrorism Act.⁵³ Other companies offer targeted “add-on” or stand-alone products geared to more specific requirements, such as the market-to-market reporting requirements in Financial Accounting Standards

permit discovery of phenomena which are “likely to be genuine” rather than “merely chance occurrences”).

⁴⁸ DAVENPORT & HARRIS, *supra* note __, at 150.

⁴⁹ *Id.* at 155.

⁵⁰ The Act also requires testimony that “the data provides a clear picture of the business, major trends, risks, and opportunities.” *See generally* TAYLOR, *supra* note __, at 31 (discussing role of systems in satisfying requirements that regulated parties not only comply with regulations, but also demonstrate that compliance).

⁵¹ Gartner Research. 2008 *Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms* (Dec. 2008) (ranking product offerings); Forrester Research, *Enterprise Governance, Risk, And Compliance Platforms, Q4 2007* (Dec. 2007) (same)

⁵² <http://www.sap.com/industries/oil-gas/large/compliance.epx>

⁵³ <http://www.sap.com/industries/consumer/large/compliance.epx>

Board (FASB) Rule 157,⁵⁴ or the European Union's REACH regulations governing reporting substance volumes and other data by the chemical industry.⁵⁵

As a whole, however, the market is converging on a unified model of "Governance, Risk and Compliance" (GRC) software intended to harmonize and unify risk and compliance activities across all business lines. Such platforms promise a means for enabling a holistic view of risk across a firm by establishing a common methodology for assessing risk data arising from the range of risk sources, by implementing procedures that mitigate risk, and by 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: (1) risk identification and measurement; (2) controls that "force" compliance with company-wide policies, including those informed by particular 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 decisionmaking authority in ways that permits fraud or obscures oversight—the type of risk illustrated most dramatically by the events resulting in \$1.47 billion in corporate losses and the 1995 bankruptcy of Barings PLC as a result of the actions of a single rogue trader operating outside of the firm's risk tolerance measures— or, on the other extreme, the risk arising from 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.

⁵⁴ See *Clearwater Analytics Automates Reporting and Disclosure Requirements to Facilitate Compliance with FAS 157*, REUTERS (Feb. 12, 2009).

⁵⁵ SAP, *New Functionality Broadens SAP's Suite of Compliance Solutions and Expands Environment, Health and Safety Offering to Reduce Chemical Industry Reporting Costs* (March 15, 2007) *available at* <http://www.sap.com/usa/industries/chemicals/large/newsevents/press.epx?pressid=7435>

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 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."⁵⁶ The technology with which Standard & Poors 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.⁵⁷ Innovations Software, which just entered into an agreement to provide risk management analysis to Fannie Mae, offers 15 computational models for credit risk assessment.⁵⁸

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

⁵⁶ http://www.oracle.com/industries/financial_services/oracle-reveleus-basel-II.html

⁵⁷ *RiskComply*, <http://www.apr.com/en/compliance/index.html>.

⁵⁸ See <http://www.innovations-software.com/fileadmin/pdf-en/success-story/credit-risk-rating-DGHYP.pdf>.

with vendors to tailor rules to their firm, or to geographic variation in regulatory requirements, a process that may become easier as software developers develop programs that automate tracking of which regulations apply to any particular transaction.⁵⁹

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. Integration of data reporting systems with operational functions can permit the uploading of information without the type of human intermediation that can permit fraud or inadvertent entry error. Automated permissions and recordkeeping 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 limit changes that can be made.

The computing power of GRC systems, moreover, brings automation one step further, aiming beyond directing what individual employees can access or do, and establishing rule systems for governing complex business decision processes themselves.⁶⁰ 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. And technology systems can develop rule-based systems that “act” upon quantitative assessments of risk, governing business-wide decisions as to 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.⁶¹

⁵⁹ A vendor called Compliance360, for example offers a “Regulatory Intelligence & Content Repository” that provides “an easily accessible, real-time view of all the activities and documentation directly linked to specific laws, regulations and other requirements,” as well as automated alerts of changes to those laws and regulations. http://www.compliance360.com/solutions_compliance_management.asp.

⁶⁰ See e.g., <http://www.fico.com/en/Products/DMTools/Pages/FICO-Blaze-Advisor-System.aspx> (discussing Fair Isaac’s leading Blaze Advisor business rules management product).

⁶¹ See, e.g., *France's Banque Populaire Group Uses Fair Isaac Rules Management Technology to Help Drive Basel II Compliance*, BUSINESSWIRE (March 31, 2004) available at

c. Monitoring Risk Management

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 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.⁶² 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,”⁶³ emphasizes the role of corporate management in monitoring risk systems and selecting risk responses. The U.S. Sentencing Guidelines, which have shaped the understanding of regulatory requirements across contexts, requires 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 caselaw governing the fiduciary duty of 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.⁶⁴

GRC systems offer the means for automating this audit and oversight function, principally by establishing baseline measurements for all major operating systems, monitoring continually the measure of 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

<http://www.allbusiness.com/banking-finance/banking-lending-credit-services/5587320-1.html>.

⁶² See 73 Fed. Reg. 13692-01, implementing certain provisions of the Gramm-Leach-Bliley Act (“GLBA”) and the Fair Credit Reporting Act (“FCRA”).

⁶³ See Committee of Sponsoring Organizations of the Treadway Commission, ENTERPRISE RISK MANAGEMENT - INTEGRATED FRAMEWORK (2004).

⁶⁴ *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

monitoring of changes in key risks. Automated systems can thus comprehensively identify both incidents inconsistent with governing rules and policies, as well as patterns that might reveal changes in risk exposure. This permits oversight both of 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.⁶⁵ This is done principally by automated periodic testing of the controls themselves, as well as continuous monitoring to “detect, after the fact, system transactions, setup, or data changes that contravene corporate policy.”⁶⁶ Vendors offer different manifestations of what they often refer to as an executive “dashboard,”⁶⁷ 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,⁶⁸ consistent with legal

⁶⁵ 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 (Sep. 1, 2007), available at http://www.cfo.com/article.cfm/9689509/1/c_2984409?f=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), available at <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.”).

⁶⁶ TARANTINO, *supra* note __, at 309.

⁶⁷ See HUGH TAYLOR, *THE JOY OF SOX* 227-28 (2006); see e.g. SAP BusinessObjects Control Process (<http://www.sap.com/solutions/sapbusinessobjects/large/governance-risk-compliance/grcprocesscontrol/index.epx>); IBM® Workplace™ for Business Controls and Reporting (<http://www-01.ibm.com/software/lotus/products/business-controls-reporting/>).

⁶⁸ See, e.g., Oracle (http://www.oracle.com/solutions/corporate_governance/integrated-financial-and-compliance-analytics.html); BWise (<http://www.bwise.com/product-suite/compliance/loss-incidents>); IBM (<http://www-01.ibm.com/software/lotus/products/business-controls-reporting/>); SAP (<http://www.sap.com/solutions/sapbusinessobjects/large/governance-risk-compliance/grcprocesscontrol/index.epx>).

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 as the types of unusual transactions that might indicate money-laundering or insider trading—or transactions that, while they may not appear out of the ordinary in and of themselves, are exceptional in comparison to other transactions made during the similar time period.

This functionality was critical in the discovery of massive fraud at Refco, the commodities and futures trading company, in 2005.⁶⁹ The firm's CEO had been hiding debts by borrowing funds 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 in 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. Automating the capacity to run monitoring tools continuously permits risk managers both to identify control failures earlier, and to 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 offer transparency into an organization's entire "risk landscape,"⁷⁰ by permitting centralized managers to view, in an updated manner, risk measures from the breadth of types of risk 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

⁶⁹ Riva D. Atlas And Jonathan D. Glater, *Mystery at Refco: How Could Such a Huge Debt Stay Hidden?*, N.Y. TIMES (Oct. 24, 2005).

⁷⁰ Klemm, *supra* note __ ("Technology can enhance visibility into an organization's risk landscape – including strategic, operational, reporting, compliance, market, credit and technology related risks.").

efficient firm organization.⁷¹ 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.⁷² 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.

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.⁷³ This effect is exacerbated in cases in which upward communications contain early tentative warnings about risk shifts;⁷⁴ 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.

71. 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.”).

72. Kirsten Foss & Nicolai J. Foss, *Authority in the Context of Distributed Knowledge* 8 (Danish Research Unit for Indus. Dynamics, Working Paper No. 03-08, 2002); Nicolai J. Foss, *Firms and the Coordination of Knowledge: Some Austrian Insights* 24–27 (Danish Research Unit for Indus. Dynamics, Working Paper No. 98-19, 1998) (discussing tacit forms of knowledge); see also MICHAEL POLANYI, THE TACIT DIMENSION 4–20 (Anchor Books 1967) (1966) (describing psychological experiments and various aspects of tacit knowledge).

73. 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 (1977) (discussing the “problems associated with the upward transmission of adverse information within the corporate hierarchy”).

74. See Langevoort, *supra* note __, at 136.

By automatically unearthing and aggregating data across business roles and functions, on the other hand, technology systems can escalate 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” that leading GRC systems feature home pages that provide executives 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.⁷⁵ 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 time,”⁷⁶ 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, enabling 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 that research on decisionmaking in organizations

⁷⁵ See also SAP BusinessObjects Process Control (<http://www.sap.com/solutions/sapbusinessobjects/large/governance-risk-compliance/grcprocesscontrol/index.epx>); IBM Workplace for Business Controls and Reporting (<http://www-01.ibm.com/software/lotus/products/business-controls-reporting/>).

⁷⁶ See generally, Steve Hamm, *IBM Roars into Business Consulting*, BUS. WEEK (Apr. 14, 2009) (discussing a test system developed by IBM, and run on one of its Blue Gene supercomputers, permitting financial-services company TD Securities to analyze options trading data in real time and make adjustments in microseconds).

demonstrates can mask the very type of risks and dangers targeted by regulation.⁷⁷

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 decisionmakers can never hope to process all available information about all possible choices, or consider the implications of every decision.⁷⁸ They 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: “biases” or “heuristics” that take cues from familiar aspects of a situation to assess unfamiliar settings, and trigger rules of decision.⁷⁹

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 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.⁸⁰ They also include “bottom-up” rules developed on the ground through the evolution of informal routines and rules of thumb. By storing organizational knowledge in this way, routines shape the lenses through which events are perceived, “allow[ing] reuse of solutions to

⁷⁷ See Bamberger, *Regulation as Delegation*, *supra* note __ at 408-435 (“Learning from the Literature on Business Organizations—How Delegation to Regulated Firms Creates Accountability Problems”).

⁷⁸. See David Hirshleifer & Siew Hong Teoh, *Limited Attention, Information Disclosure, and Financial Reporting* 5–9 (Dec. 20, 2002), <http://www.cob.ohio-state.edu/fin/dice/papers/2002/2002-5.pdf> (reviewing the theory and evidence on limited attention and information processing).

⁷⁹. HERBERT A. SIMON, *ADMINISTRATIVE BEHAVIOR* xxix (3d ed. 1976) (setting forth the understanding that, rather than “maximizing,” humans consider only a few possible courses of action and “satisfice[],” choosing to settle for a solution that is adequate)

⁸⁰. RICHARD M. CYERT & JAMES G. MARCH, *A BEHAVIORAL THEORY OF THE FIRM* 134 (Blackwell Publishers 1992) (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.”).

problems,”⁸¹ which in turn allows organizations to find “good, even optimal, rules for many choices they are likely to face.”⁸²

Yet this organizational source of strength can also create predictable decisionmaking pathologies, by rendering decisionmakers insensitive to change, the source of risk. These knowledge structures accentuate familiarity—what is cognitively “available”⁸³—and deemphasizes 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.⁸⁴ In this way, individuals unconsciously “make the problematic non-problematic”⁸⁵ 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

81. MARCH, SCHULZ & ZHOU, *supra* note __, at 186 (“[O]rganizations confront internal and external problems, draw inferences from their experiences in those confrontations, and encode the inferences in rules. Lessons encoded in rules represent knowledge about solutions to problems found in the past. Rules retain knowledge and allow reuse of solutions to problems.”).

82. *Id.*

83. 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 “availability heuristic”).

84. 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); Hillel J. Einhorn & Robin M. Hogarth, *Confidence in Judgment: Persistence of the Illusion of Validity*, 85 PSYCHOL. REV. 395 (1978); Jonathan St. B.T. Evans, *Beliefs and Expectations as Causes of Judgmental Bias*, in JUDGMENTAL FORECASTING 31 (George Wright & Peter Ayton eds., 1987); Barry M. Staw, *The Escalation of Commitment to a Course of Action*, 6 ACAD. MGMT. REV. 577 (1981). For discussions of predecisional distortions of information, see generally Aaron L. Brownstein, *Biased Predecision Processing*, 129 PSYCHOL. BULL. 545 (2003); J. Edward Russo et al., *The Distortion of Information During Decisions*, 66 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 102 (1996) (reporting findings of predecision distortions).

85. Vaughan, *supra* note __, at 280–81.

institutions.⁸⁶ 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.⁸⁷ This permits decisionmakers the self-deception that the group interest is "in full consistency with their personal goals."⁸⁸ 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.⁸⁹ 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 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.⁹⁰

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 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.

⁸⁶ 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 (1997).

⁸⁷ *Id.* at 144 ("The notion of self-serving inference is another fundamental construct in social cognition."). For other discussions of self-serving bias, see Linda Babcock & George Loewenstein, *Explaining Bargaining Impasse: The Role of Self-Serving Biases*, 11 J. ECON. PERSP. 109 (1997); Jolls et al., at 1501–04; Jeffrey J. Rachlinski, *The Uncertain Psychological Case for Paternalism*, 97 NW. U. L. REV. 1165, 1172–73 (2003).

⁸⁸ Langevoort, *supra* note __, at 144.

⁸⁹ *Id.* at 141.

⁹⁰ *Id.* at 106.

⁹¹ 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,”⁹² which dominant knowledge structures might mask as anomalous, yet may be the best indicators of risk.⁹³

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.⁹⁴ That system’s predictive risk analytic methods, and tests of risk exposure such as scenario analysis and stress testing,⁹⁵ 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.⁹⁶ 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 hurt, despite the fact that it held \$13.98 billion in collateralized debt obligations written by AIG.⁹⁷

⁹¹ See Carla O’Dell & C. Jackson Grayson, *If Only We Knew What We Know: Identification and Transfer of Internal Best Practices*, 40 CAL. MGMT. REV. 154, 157 (1998) (contrasting internal benchmarking with “[o]rganizational structures that promote ‘silo’ behavior”).

⁹² C. Marlene Fiol & Edward J. O’Connor, *Waking Up! Mindfulness in the Face of Bandwagons*, 28 ACAD. MGMT. REV. 54, 63 (2003).

⁹³ See Karl E. Wieck et al., *Organizing for High Reliability*, 21 ORG. BEHAV. 81, 92 (1999) (discussing how mindful organizations create processes to view localized failure as a sign of generalizable problems).

⁹⁴ See sources at *supra* note ____.

⁹⁵ Nina Mehta, *One on One Interview With Emanuel Derman*, Financial Engineering News, July/Aug. 2003 (in which former Goldman Sachs risk modeler Emanuel Derman said, “In a good way, Goldman Sachs was eclectically irreligious 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.”) (available at <http://www.ederman.com/new/docs/fen-interview.html>).

⁹⁶ Joe Nocera, *Risk Mismanagement*, N.Y. Times, Jan. 4, 2009.

⁹⁷ *Heard on The Street: Goldman’s Price of Protection*, Wall St. J., March 18, 2009, at C4 (“If Goldman were able to withstand the bankruptcy of a large counterparty like 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.⁹⁸ 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, to those that are event-triggered, such as data regarding banking losses, or the “Suspicious Activity Reports” required by the Bank Security Act and the U.S. Patriot Act within 30 days of discovery of transactions flagged under metrics intended to track internal abuse or money-laundering.⁹⁹

For large firms especially, and for an increasing number of small and medium entities, such requirements require 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 necessitate 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

III. 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

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.”)

⁹⁸. 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. *See generally* Cass R. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613 (1999) (discussing those compelled disclosures that are meant to affect market responses and those meant to affect political responses).

⁹⁹ *See* 31 C.F.R. § 103.18.

be met by manual processes, or even stand-alone spread-sheet 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.

As scholars of information technology have described, such technology functions, itself, as a “newly salient regulator;”¹⁰⁰ its software code functions as “law.”¹⁰¹ 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.”¹⁰²

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.¹⁰³ 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] enlist? Do the ways risk management regimes have developed sufficiently improve the responsiveness of corporate decisionmaking 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.¹⁰⁴ By setting standards that regulated entities must achieve,

¹⁰⁰ LESSIG, *supra* note __ at 6 (“[Cyberspace] compels us to look beyond the traditional lawyer’s scope—beyond laws, regulations, and norms. It requires an account of a newly salient regulator.”). *See also id.* at 5 (“Cybernetics had a vision of perfect regulation. Its very motivation was finding a better way to direct.”)

¹⁰¹ Reidenberg, *supra* note __ at 553.

¹⁰² Grimmelman, *supra* note __, at 1732.

¹⁰³ LESSIG, *supra* note __ at 324.

¹⁰⁴ *See* Thomas O. McGarity, *Radical Technology-Forcing in Environmental Regulation*, 27 *LOY. L.A. L. REV.* 943 (1994); Jerry L. Mashaw & David L. Harfst, *Regulation and Legal*

public legal 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 that 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 I, largely do not.

Moreover, although regulators recognize formally that the management-based mandates they promulgate regarding financial and operational risk necessitate a turn to technology,¹⁰⁵ they have, with few

Culture: The Case of Motor Vehicle Safety, 4 YALE J. ON REG. 257 (1987) (discussing the concept of technology forcing); Richard B. Stewart, *Regulation, Innovation, and Administrative Law: A Conceptual Framework*, 69 CAL. L. REV. 1256 (1981); Russell V. Randle, *Forcing Technology: The Clean Air Act Experience*, 88 YALE L.J. 1713 (1979); see also Peter S. Menell paper; Gideon Parchomovsky & Alex Stein, *Torts and Innovation*, 107 MICH. L. REV. 285 (2008).

¹⁰⁵ See, e.g., FED. RESERVE SYS., TRADING AND CAPITAL MARKETS ACTIVITIES MANUAL, 2040.1, 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 AND REGULATION, LETTER SR 00-3 (Feb. 2000) (“Banking organizations increasingly rely on information technology to conduct their operations and manage risks.”); OFFICE OF THE COMPTROLLER OF THE CURRENCY, BULL. NO. 98-3, TECHNOLOGY RISK MANAGEMENT, 4 (1998) (on file with author) (“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.ffiec.gov/ffiecinfobase/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, THRIFT ACTIVITY HANDBOOK 341.2 (on file with author) (“Financial institutions have a number of choices available to meet their information systems and technology needs.”).

exceptions,¹⁰⁶ 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” models (discussed further in Part III) relying on historical data that many GRC systems incorporate.¹⁰⁷ Individual financial institution regulators have, moreover, periodically exercised their soap-box 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, including 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.”¹⁰⁸ 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 the “new governance” approach’s imagery of the government 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 policymakers. In turn, it overlooks the challenge posed by compliance choices for both effective regulation and legitimate public administration.

¹⁰⁶ These exceptions, such as certain activities of the Federal Trade Commission and Food and Drug Administration discussed in part IV as models for innovation, *see* text at nn. ___-___, occur largely outside the financial-regulation context.

¹⁰⁷ *See, e.g.*, 17 C.F.R. § 229.305(a)(iii)(A) (provisions regarding “Quantitative and qualitative disclosures about market risk,” in standard SEC filings).

¹⁰⁸ Susan Schmidt Bies, *Enterprise Risk Management and Mortgage Lending*, Speech at the National Credit Union Administration 2007 Risk Mitigation Summit (Jan. 11, 2007), *available at* <http://www.federalreserve.gov/newsevents/speech/bies20070111a.htm>.

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 II, technology systems can reasonably be described, as they are by regulators, vendors and users, as powerful managerial “tools,”¹⁰⁹ that management can “tailor[]” to organizational needs and “universal compliance”; which are “flexible to respond to change” and which increase visibility and oversight of business processes.

Research into information systems, however, suggest 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, posing 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, in that technological choices “embody biases that exist independently, and usually prior to the creation of the system.” And they rise 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; imperfections in pseudorandom number

¹⁰⁹ Patrick Feng, *Rethinking Technology, Revitalizing Ethics: Overcoming Barriers to Ethical Design*, 6 SCI. & ENG. ETHICS 207, 210 (2000).

generation; and the attempt to make human constructs amenable to computers.”¹¹⁰

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.

This process leads to numerous winnowing effects as to the breadth and nature of risk identification. The necessity to develop “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 measured¹¹¹—as well as towards existing types of metrics. As such, it 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,¹¹² and embrace prevailing disciplinary notions—spread through business schools, industry associations, and consulting firms—of what types of risk can be quantified and measured.

This bias is exacerbated by the attempt to integrate legal with management ideas regarding the types of controls that can manage risk. To begin with, business rules are poor vehicles for capturing nuance in legal policy,¹¹³ especially in a context like risk management, in which regulators have eschewed rules for standards. Moreover, the focus on internal controls as a mechanism for legal compliance, however useful it may be, can further skew the viewpoint of risk assessment towards backwards-looking metrics, for “Control actions are based on feedback from a disturbance that *has occurred*], while risk, by contrast, is about *future* disturbances.”¹¹⁴

¹¹⁰ Batya Friedman and Helen Nissenbaum, *Bias in Computer Systems*, 14 ACM TRANSACTIONS ON INFO. SYS. 330, 335 (1996) (discussing “preexisting bias” and technical bias”).

¹¹¹ See Tobias Scheytt, *et al.*, *Organizations, Risk and Regulation*, 43 J. MANAGEMENT STUDS., 1331, 1333 (2006) (“[D]eeply rooted ideas about the ways in which risk is ‘normally’ handled inform the organization of cognition by accounting and information systems.”) (quoting KARL E. WEICK, *SENSEMAKING IN ORGANIZATIONS* (1995)).

¹¹² See Claudio Ciborra, *Imbrication of Representations: Risk and Digital Technologies*, 43 J. MANAGEMENT STUDS. 1339 (2006).

¹¹³ See Danielle Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249, 1261 (2008).

¹¹⁴ Ciborra, *Imbrication of Representations*, *supra*, note ___, at 1346.

These distortions, finally, are compounded when “requirements” reflecting salient sources of risk, approaches to their measurement, and controls for their mitigation, are turned over to experts, of both the programmer and “quant” varieties, for translation into predictive algorithms and computer code.¹¹⁵ These experts may know nothing of the management of risk within organizations, or of the law.¹¹⁶ 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.”¹¹⁷ 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.¹¹⁸

The choice will also be shaped by practical constraints on computing capacity and system cost. The case of Goldman Sachs’ 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. The unlikely occurrence of ten independent daily loss reports revealed an unlikely “red flag” that a weekly reporting system would only have considered a single

¹¹⁵ TAYLOR, SMART (ENOUGH) SYSTEMS, *supra* note __, 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.”).

¹¹⁶ See Danielle Citron, *supra* note __, 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, “[t]o 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).

¹¹⁷ Friedman & Nissenbaum, *supra* note __.

¹¹⁸ Jay P. Kesan & Rajiv C. Shah, *Deconstructing Code*, 6 Yale J. L. & Tech. 277 (2004).

loss event. Yet real-time calculations require massive computing power; IBM's touted recent test system permitting a small financial-services company to analyze options trading data in real time is housed on one of the computing giant's Blue Gene supercomputers,¹¹⁹ computers developed to surpass all existing processing speeds.¹²⁰

Moreover, like any choice to govern by rule rather than standard, the ultimate choice will inevitably result in inexactness; it will be, in different ways, both over- and under-inclusive.¹²¹ 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[] rel[iance] 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 that:

[i]f 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.¹²²

¹¹⁹ See Steve Hamm, *IBM Roars into Business Consulting*, BUS. WEEK (Apr. 14, 2009).

¹²⁰ *Compare Ambit Case Study*, EXPERIENCE 51-52 (detailing Connecticut's Webster Bank's Risk Management system providing monthly models analyzing loan and interest rate risk).

¹²¹ See, e.g., V. Fon & Francesco Parisi, *On the Optimal Specificity of Legal Rules*, 3 J. INSTITUTIONAL ECON. 147 (2007); see generally, 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).

¹²² U.S. Securities and Exchange Commission, *Speech by SEC Staff: Remarks before the NRS 21st Annual Spring Compliance Conference by John H. Walsh Associate Director - Chief Counsel Office of Compliance Inspections and Examinations* (Apr. 18, 2006), available at <http://www.sec.gov/news/speech/2006/spch041806jhw.htm>

For this reason, even business or legal “rules which appear superficially simple to represent formally [in computer code] may give rise to latent complications once legal contextual issues are considered.”¹²³

In these ways, the process of technological translation of legal mandates governing risk management encounters a “many hands problem.”¹²⁴ 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”¹²⁵ is that no expert system can be wholly authoritative in the consequences of its expert principles, 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, resistant to detection or repair. To be sure, the purveyors of technology solutions tout their plasticity¹²⁶—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.¹²⁷ Such path dependence transforms it, in the words of one socio-technical

¹²³ Harry Surden *et al.*, *Managing Representational Complexity in Computational Law*; J.C. Smith, *An Introduction to Artificial Intelligence and Law: or, Can Machines be Made to think like Lawyers?*, available at <http://www.flair.law.ubc.ca/jcsmith/logos/noos/machine.htm>.

¹²⁴ See Helen Nissenbaum, *Accountability in a Computerized Society*, in BATYA FRIEDMAN, ED., *HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY* 40 (1997) (discussing the ways in which the “problem of many hands” erodes accountability in computerized societies); Claudio U. Ciborra, *De profundis? Deconstructing the concept of strategic alignment*, 9 *SCAND. J. INFOR. SYS.*, 67 (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.”)

¹²⁵ ANTHONY GIDDENS, *CONSEQUENCES OF MODERNITY* (1991) (detailing the “risk profile” of modernity).

¹²⁶ Grimmelmann *supra*, note __ (quoting FREDERICK BROOKS, *THE MYTHICAL MAN MONTH* (1975), describing software architecture: “Few media of creation are so flexible, so easy to polish and rework, so readily capable of realizing grand conceptual structures.”).

¹²⁷ Langdon Winner, *Do artifacts have politics*, in, *THE SOCIAL SHAPING OF TECHNOLOGY: HOW THE REFRIGERATOR GOT ITS HUM* (Donald MacKenzie and Judy Wajcman, eds.), at 29 (1985).

scholar, from a device “oriented toward human needs,” into “an important component [] of the formative context.”¹²⁸ This characteristic, too, tracks code’s function as “law”: technology is “similar to legislative acts or political foundlings that establish a framework for public order that will endure for many generations.”¹²⁹

This systematization of initial patterns persists for technical, institutional and cognitive reasons. While computer code and predictive analytics methods might be accessible to programmers, they remain opaque to users, for whom it is often only outcomes that remain visible.¹³⁰ Programmers “code[] layer after layer of policies and other types of rules” that managers and directors cannot hope to understand or unwind¹³¹—a phenomenon exacerbated by the prevalence of off-the-shelf GRC products and risk analytics—while “[t]he ability to do [understand] complex financial instruments requires literally a Ph.D. in applied mathematics.”¹³² 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.”¹³³

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.”¹³⁴ In the case of GRC systems, this representational power of

¹²⁸ Ciborra, *De profundis?*, *supra* note __

¹²⁹ Winner, *supra* note __ at 29.

¹³⁰ Grimmelman, *supra* note __, at 1732 (“That programmers have such flexibility does not necessarily mean that users do. Our hypothetical programmer could easily choose to make her calculator program use decimal notation, scientific notation, or both. But once she has made that choice, the user cannot easily undo it. When users are powerless over software, it is often because programmers have made design decisions that leave users without power. Indeed, this imbalance is part of the effectiveness of regulation by software.”).

¹³¹ Citron, *supra* note __, at 1304. (“Different programmers might have coded layer after layer of policies and other types of rules in various ways. Some companies have tens of thousands of rules coded into their systems....”)

¹³² *The un-Gilded Age*, Brilliantleap.com (Oct. 1, 2008), available at http://brilliantleap.com/blog/2008/10/the_ungilded_age.html

¹³³ PricewaterhouseCoopers survey, at <http://www.boardmember.com/media/files/research-pdfs/WDTResults2008.pdf>.

¹³⁴ MARTIN HEIDEGGER, *THE QUESTION CONCERNING TECHNOLOGY* 57 (1977) (describing the notion of “*Gestell*”); see CLAUDIO CIBORRA, *THE LABYRINTHS OF INFORMATION: CHALLENGING THE WISDOM OF SYSTEMS*, Ch. 4 (2002) (exploring Heidegger’s notion in the context of information systems).

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. Humans judgment is subject to an “automation bias,” which fosters a tendency to “disregard or not search for contradictory information in light of a computer-generated solution that is accepted as correct.”¹³⁵ 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.¹³⁶ 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, increasing instead individual decisions that maximize personal earnings.¹³⁷ Thus the benefits of machine “judgment” may come at the cost of human decisionmaking 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

¹³⁵ Mary .L. Cummings, *Automation and Accountability in Decision Support System Interface Design*, 32 J. TECHNOL. STUD. 23, 27 (2006); see also, e.g.,

¹³⁶ Eugenio Alberdi, *et al.*, *Automation Bias In Medical Decision Making: A Study With Incorrect Computer Prompting In Breast Cancer Screening*, PROC. 27TH ANNUAL MEETING OF THE SOCIETY FOR MEDICAL DECISION MAKING (SMDM05), (2005) (finding that the first group identified 46% of the cancers unmarked by the program, while the second group identified 88% of the total cancers).

¹³⁷ Steven T. Schwartz and David E. Wallin, *Behavioral Implications of Information Systems on Disclosure Fraud*, 14 BEHAV. RES. IN ACCOUNTING (2002); see also generally, Shigeyuki Goto, *The Bounds of Classical Risk Management and The Importance of a Behavioral Approach*, 10 RISK MGMT. & INSURANCE REV. 267 (2007).

masks areas where risk types are ignored or analysis is insufficient, and where more revolutionary, paradigm-shifting advances might be warranted.¹³⁸

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 that other firms adopt, seeking legitimacy.¹³⁹ 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.¹⁴⁰

By these phenomena of representation and institutionalization, technology systems developed to manage risk in turn become sources of risk themselves.¹⁴¹ They create the perception of stability through probabilistic reasoning, and the experience of accuracy, reliability, and comprehensiveness through automation and presentation, drawing 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 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

¹³⁸ See generally, J.S. Busby, *Failure to Mobilize in Reliability-Seeking Organizations: Two cases from the UK railway*, 43 J. MGMT. STUD. 1375 (2006) (providing case studies illustrating that “[i]f 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”).

¹³⁹ See Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOC. REV. 147, 150, 152 (1983); 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.”).

¹⁴⁰ See Lauren B. Edelman et al., *The Endogeneity of Legal Regulation: Grievance Procedure as Rational Myth*, 105 AM. J. SOC. 406 (1999); Lauren B. Edelman et al., *Internal Dispute Resolution: The Transformation of Civil Rights in the Workplace*, 27 LAW & SOC’Y REV. 497, 529 (1993); cf. Warren Buffet: “the five most dangerous words in business are: Everyone else is doing it.”

¹⁴¹ Scheytt, *et al.*, *supra* note ___ (describing how “stable climates of probabilistic reasoning in risk management are challenged by the transformation of side-effects into new risk ‘objects’”)

and unwieldy legal mandates and market expectations.¹⁴² Technology systems, accordingly, create the systemic preconditions for the “integral accident,” the notion that with the creation of each invention, that invention's “accident” is also simultaneously created.¹⁴³

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.¹⁴⁴ Internal organizational incentive structures, especially in industries generating the types of instability policymakers seek to reduce, frequently reward the type of abnormal successes that can arise from undesirably risky behavior.¹⁴⁵ 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 masks its riskiness from technological sensitivity. Layers of technological opacity, moreover, can shield such behavior from both internal and external oversight until negative outcomes have manifest themselves. Thus systems intended to identify exceptions can, in the hands of those familiar with them, serve to shield remarkable behavior.

5. *Technology Failures and the Financial Crisis*

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, and corresponding assessments or risk increasingly tacked to analytics that embedded certain hypothesis,

¹⁴² See EUGENE BARDACH & ROBERT A. KAGAN, *GOING BY THE BOOK: THE PROBLEM OF REGULATORY UNREASONABLENESS* 64–66 (1982) (arguing that most regulated enterprises are “good apples” who 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).

¹⁴³ PAUL VIRILIO, *THE ORIGINAL ACCIDENT* (2007); see also Charles Perrow, *Power* (2005).

¹⁴⁴ See Erik F. Gerding, *Code, Crash, and Open Source: The Outsourcing of Financial Regulation to Risk Models and the Global Financial Crisis*, *Wash. L. Rev.* (forthcoming 2009) (discussing the ways that individuals “adapt to the set of legal rules designed to constrain their behavior,” and explaining that “one adaptive response is to game risk models”).

¹⁴⁵ See generally Kimberly D. Krawiec, *The Return of the Rogue*, 51 *ARIZ. L. REV.* 127 (2009) (describing how such incentives thwart enforced self-regulatory regimes such as Basel II); Kimberly D. Krawiec, *Accounting for Greed: Unraveling the Rogue Trader Mystery*, 79 *Or. L. Rev.* (describing the benefits of “rogue trading” to firms and traders).

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 loans into an asset-backed securities, or collateralized debt obligations (CDOs) which were then used as collateral against further loans.

The unregulated, and non-standardized, 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 risk of payment due to default in the underlying debt. Yet as CDSs were issued for highly-leveraged, and increasingly uncertain, derivative products, these investments no longer had a known entity to follow to determine the strength of a particular loan or bond (as in the case of CDSs for commercial loans, corporate bonds or municipal bonds).

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 necessary for compliance with reserve and capital requirements. Accordingly, they sought to stretch analytics embedded in established risk management systems to new contexts.

In particular, they applied the technological systems institutionalized for calculating the short-term risk of traditional financial holdings—and the “Value at Risk” approaches on which they relied—to calculate the level of risk inherent in the unregulated CDO and CDS markets. Value at Risk (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. 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.

Value at Risk 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.” 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. VaR approaches reach their calculation generally 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, 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 (like scientific phenomena like fluids and cellular structure), which simulates the multiple sources of uncertainty affecting an asset’s value, 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 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.¹⁴⁶ These would provide the technological basis for what former Morgan CEO Dennis Weatherstone called the “4:15 report”—a one-page firm risk report available 15 minutes after the market’s close.¹⁴⁷

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.

¹⁴⁶ See *Company History*, <http://www.riskmetrics.com/history> (providing the history of the company RiskMetrics, which began as an internal risk management function of J.P. Morgan and developed the VaR model in 1994).

¹⁴⁷ See *id.*

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 from computer screens¹⁴⁸ to provide daily assessments of liquid “Level I” assets¹⁴⁹, 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—and assets, moreover, whose value was tied not to market data, but to “non-observable 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.¹⁵⁰

Perhaps more shockingly, in the six months before its meltdown, AIG did not have either a full-time CFO or chief risk-assessment officer.¹⁵¹ 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.¹⁵² Indeed, according to the findings of the SEC’s Inspector General, given their “lack of expertise in mortgages, it would have been

¹⁴⁸ See Caitlyn Zaloom, *Markets and Machines: Work in the Technological Sensoriscapes of Finance*, 58 AM. Q. 815-(2006).

¹⁴⁹ FINANCIAL ACCOUNTING RULE 157.

¹⁵⁰ Nancy Stein, *Prof. John Coffee on the Crisis*, LAWDRAGON, available at http://www.lawdragon.com/index.php/newdragon/fullstory/prof_john_coffee_on_the_crisis.

¹⁵¹ Matt Taibbi, *The Big Takeover*, ROLLING STONE (Mar. 19 2009), available at http://www.rollingstone.com/politics/story/26793903/the_big_takeover/print

¹⁵² U.S. Securities and Exchange Commission, Office of the Inspector General, Office of Audits, *SEC’s Oversight of Bear Stearns and Related Entities: The Consolidated Supervised Entity Program*, Report No. 446-A (Sep. 25, 2006), available at <http://finance.senate.gov/press/Gpress/2008/prg092608i.pdf>.

difficult for risk managers at Bear Stearns to advocate a bigger focus on default risk in its mortgage models.”¹⁵³ 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 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.”¹⁵⁴

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.¹⁵⁵ 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.¹⁵⁶ 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 well 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 the immeasurable with great precision” permitted regulated firms to present regulators with quantitative “evidence” of compliance with risk management mandates and capital reserve requirements,

¹⁵³ *Id.*

¹⁵⁴ See Gerding, *supra* note __ (quoting Nocera, *supra* note __, at 46).

¹⁵⁵ See Taleb, *supra* note __ (discussing the use of financial technology “to quantify the immeasurable with great precision”).

¹⁵⁶ VaR is thus geared towards measurement of “Knightian risk” involving situations where probabilities are given, but not towards “Knightian uncertainty,” which refers situations in which possible outcomes can be identified but probabilities are not measurable, (Knight, 1921), or towards situations involving “Structural ignorance,” where outcomes are neither naturally given nor easily constructed by the decision-maker (Gilboa and Schmeidler, 2001).

especially after those obligations were reduced by the SEC in 2004.¹⁵⁷ It 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 percent chance that AIG would never have to pay out on the CDSs it executed,¹⁵⁸ while the credit rating agencies' ultimate downgrading of AIG's AAA rating to AA was completely unrelated to these products). And it 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,¹⁵⁹ while 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."¹⁶⁰

C. 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

¹⁵⁷ See Stephen Labaton, *Agency's '04 Rule Let Banks Pile on New Debt*, N.Y. TIMES (Oct. 2, 2008).

¹⁵⁸ See Robert O'Harrow & Brady Dennis, *A Crack in the System*, WASH. POST, Dec. 30, 2008, at A01. 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 case of a full-blown depression, in which case the counterparties would go bankrupt and would not likely demand payment, *see id.* See also SEC Form 10-K, *American International Group, Inc.* (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."), *available at* <http://www.sec.gov/Archives/edgar/data/5272/000095012308002280/y44393e10vk.htm#113>.

¹⁵⁹ Robert O'Harrow Jr. & Jeff Gerth, *As Crisis Loomed, Geithner Pressed But Fell Short*, WASH. POST (April 3, 2009).

¹⁶⁰ *The Bet That Blew Up Wall Street: Steve Kroft On Credit Default Swaps And Their Central Role In The Unfolding Economic Crisis*, 60 MINUTES (Oct. 26, 2008), *available at* <http://www.cbsnews.com/stories/2008/10/26/60minutes/main4546199.shtml>.

decisionmaking in ways that “drift” significantly from those ends, raising issues of both effective governance and legitimate public administration.

Technology-based compliance systems proliferate in contexts in which policymakers have rejected rule-based mandates, and instead employed 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: that choices will be shaped by both 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 dynamic nature of systems will shape perception and judgment in ways that produce decisions unmoored from intention and objective.

Moreover, 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 oversight,¹⁶¹ masking important 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 then rely on the resulting conclusions about risks and safeguards offered them by the parties they regulate.

These sorts of systemic effects indicate, at least, that the reluctant-regulator model of 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 can be literally arbitrary (in that they reflect factors that relevant decisionmakers do not intend to matter),¹⁶² captured by a variety of private concerns, and unaccountable, with significant potential for social harm.

¹⁶¹ *In re: Caremark* (“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 a corporations operations without doing so.); Sarbanes Oxley officers requirements.

¹⁶² In the words of the Supreme Court, the arbitrary—and therefore illegitimate—exercise of delegated discretion, is that which “relie[s] on factors which Congress [or agencies] ha[ve] not intended,” has “entirely failed to consider an important aspect of

IV. PROPOSALS FOR REFORM

In light of technology's capacity on the one hand, and the dangers of overreliance on technology systems on the other, this Section 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 better to reflect the human decisionmaking element at both levels: the ways human judgment can be skewed by technology; methods for reintroducing such 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 from the 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 the ability to react to "disloyal" activities—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 greater visibility into regulators' conceptions as to meaningful satisfaction of risk management mandates, promoting both effective public management, and important rule-of-law and accountability values.

If purely top-down regulatory 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

the problem [or] offered an explanation for its decision that runs counter to the evidence," 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).

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.”¹⁶³ Such an “amended account” is instead “both top-down and bottom-up.”¹⁶⁴

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 while systems theory predicts that regulated parties will adapt to a static set of external rules with a minimum of change – resulting only in by “cosmetic” trappings of compliance¹⁶⁵ – a dynamic model of regulation creates a “continuous stimulus” that must be translated into meaningful internal practice.¹⁶⁶

What might this model suggest in the context of technological risk management—and what advice might it offer policymakers revisiting the administrative institutions and policy approaches that failed to

¹⁶³ Michael Dorf, *The Domain of Reflexive Law*, 103 Colum. L. Rev. 384, 384 (2003) (reviewing Jean Cohen, *Regulating Intimacy: A New Legal Paradigm* (2002)); see also Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 Colum. L. Rev. 267, 322 (1998); Bradley C. Karkkainen et al., *After Backyard Environmentalism: Toward a Performance-Based Regime of Environmental Regulation*, 44 AM. BEHAV. SCIENTIST 692, 692–709 (2000) (providing, in the environmental context, a model in which administrative agencies develop the architecture for gathering and analyzing information across local contexts as a part of the regulatory and education process); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342 (2005) (providing an account of this body of scholarship).

¹⁶⁴ Dorf, *supra* note ___, at 384.

¹⁶⁵ Kimberly D. Krawiec, *Cosmetic Compliance and the Failure of Negotiated Governance*, 81 WASH. U. L.Q. 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 Kimberly D. Krawiec, *Organizational Misconduct: Beyond the Principal-Agent Model*, 32 FLA. ST. U. L. REV. 571 (2005) (arguing that organizations have perverse incentives to implement ineffective compliance programs); see also Bamberger, *Regulation as Delegation*, 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.”).

¹⁶⁶ Edward L. Rubin, *Images of Organizations and Consequences of Regulation*, 6 THEORETICAL INQUIRIES IN L. 347, 387 (2005); see *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.”)

ensure that mandated risk management prevented systemic financial meltdown?

A. 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 such systems themselves currently claims little regulatory traction. To be sure, a number of regulatory regimes nod towards the 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, a process which requires that regulated entities describe of the elements they intend to consider in such an approach.¹⁶⁷ Moreover, the third of the three “pillars” undergirding the Basel framework is “market discipline through enhanced public disclosures.”¹⁶⁸ 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 “the scope and nature of risk reporting and/or measurement systems.”¹⁶⁹

The regulations implementing Basel II themselves make clear, however, that banks are provided “with considerable discretion with regard to public disclosure requirements.”¹⁷⁰ Thus not only do the

¹⁶⁷ Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version* 148-154 (2006).

¹⁶⁸ U.S. Department of the Treasury, Office of the Comptroller of Currency, *Risk-Based Capital Standards: Advanced Capital Adequacy Framework -- Basel II*, 72 Fed. Reg. 69288 (Dec. 7, 2007), *codified at* 12 C.F.R., Part 3.

¹⁶⁹ *Id.* See also *id.* at Table 11.3 (“Capital Adequacy”) (requiring “[a] summary discussion of the . . . approach to assessing the adequacy of its capital to support current and future activities”); and *id.* at Table 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.”)

¹⁷⁰ *Id.*

advanced risk-measurement approaches permitted by the Basel II framework accord financial services firms significant flexibility in their assessment methodologies – with no standardized method for measuring, weighing and integrating the methods for assessing risk.¹⁷¹ They also let bank management “determine[] which disclosures are relevant based on a materiality concept,” according “flexibility regarding formatting and the level of granularity of disclosures.”¹⁷² Such discretion is heightened further, moreover, “if a bank believes that disclosure of specific commercial or financial information would prejudice seriously 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.”¹⁷³

Not surprisingly, several recent studies of risk management transparency reveal that “disclosures related to the subject apparently still have a long way to go.”¹⁷⁴ Such disclosures lack the type of detail about the risk-assessments analytics used that would permit meaningful assessment of internal controls, or the sort of standardization that would

¹⁷¹ While a sound “advanced measurement” framework considers four sources of information: (1) internal operational risk loss data; (2) relevant external operational risk loss data; (3) scenario analysis of expert opinion; (4) and bank-specific business environment and internal control factors, see Jean-Phillippe Peters and Georges Huebner, *Modeling Operational Risk Based on Multiple Experts’ Opinions*, in GREG N. GREGORIOU, ED., OPERATIONAL RISK TOWARD BASEL III: BEST PRACTICES AND ISSUES IN MODELING, MANAGEMENT, AND REGULATION (2009), at 4, the Basel II framework leaves discretion as to how to combine them, and there are neither formal, nor generally accepted, methodologies for their reporting, see Guy Ford, et al., *Operational Risk Disclosure in Financial Services Firms*, in GREG N. GREGORIOU, ED., OPERATIONAL RISK TOWARD BASEL III: BEST PRACTICES AND ISSUES IN MODELING, MANAGEMENT, AND REGULATION (2009), at 384.

¹⁷² *Id.*

¹⁷³ *Id.* The SEC’s Regulation S-K thus requires disclosure of only “description[s]” of underlying financial models used in assessing in periodic financial filings. See, e.g., 17 C.F.R. § 229.305(a)(ii)(B) (providing that “[r]egistrants shall provide a description of the model, assumptions, and parameters”); 17 C.F.R. § 229.305(a)(iii)(B)(1)(i-ii) (requiring provision of “[t]he average, high and low amounts, or the distribution of the value at risk amounts for the reporting period”

¹⁷⁴ Melissa Klein Aguillar, *Report: Disclosures on ERM Lacking*, COMPLIANCE WK. (June 30, 2009) (summarizing a study of 4162 companies GovernanceMetrics International finding a lack of standardized disclosure—and often of any disclosure—of company-wide risk management), see http://www.gmiratings.com/Release_GMI_Boards_Risk_Oversight_6_29_09.pdf; see also,

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 potential for transparency as to the exact methods of quantifying risk and the ways such measures automate decisionmaking; and second, 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 for the standardization of 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. Standardized requirements would mandate the detailed submission of both the code and operational specifics of compliance technology systems to regulators, 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, or those targeted submissions required by the Federal Reserve Bank for stress-testing of certain large banks in the wake of the financial crisis. Requiring such granularity in reporting can promote transparency to regulators, but also to firm managers, who themselves may not possess full familiarity with the choices embedded by third parties 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.¹⁷⁵ 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.¹⁷⁶

Moreover, the ability to combine standardized approaches with enhanced public disclosure of certain elements of risk information can

¹⁷⁵ See generally, Kenneth A. Bamberger, *Proprietary Law: Trade Secrets and Regulatory Disclosure* (work in progress).

¹⁷⁶ See generally, Joseph Lorenzo Hall, *Policy Mechanisms for Increasing Transparency in Electronic Voting*, (Unpublished Ph.D. Dissertation, UC Berkeley School of Information (2008) (discussing policy mechanisms for promoting disclosure of computer code underlying voting technology).

enlist robust input and oversight by third parties, including investors, analysts, academics and non-profits.¹⁷⁷ 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, or XBRL, format for data contained in filings with the agency.¹⁷⁸ While confidentiality and 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 to date tilted too far in the direction of secrecy. In its recent establishment of a "Transparency Task Force," it has embraced the goal of making "useful and understandable information available to the public in a timely and user-friendly fashion,"¹⁷⁹ a goal that can leverage private regulatory oversight considerably.

B. 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. Regulators constrained by limited resources cannot currently keep up with the massive data processing capacity of private corporations.¹⁸⁰ Many have not developed staff capacity for robust analysis of analytic approaches employed by those firms. And even when agency staff claim technical expertise, institutional structures may not be geared to promote the independence in analysis of technological approaches necessary to probe meaningfully into the institutionalized, and static assumptions underlying accepted risk management practices. Indeed, especially if an agency draws its technologically-sophisticated staff from a pool that shares training and experience with those

¹⁷⁷ Erik Gerding in fact argues that such technology should be fully "open source," see Gerding, *supra*, note ____.

¹⁷⁸ See Final Rule: Interactive Data to Improve Financial Reporting, 17 C.F.R. §§ 229, 230, 232, 239, 240 & 249 (effective Apr. 13, 2009) (setting forth a three-year, phased-in implementation schedule for various types of companies); *Interactive Data Previewer and Rendering Engine* at <http://www.sec.gov/xbml> (providing the source code); Kate Plourd, *SAP Plays the Data Tagging Game*, CFO Magazine (Feb. 20, 2009) available at http://www.cfo.com/article.cfm/13144083/c_2984312/?f=archives (documenting efforts of major GRC vendors like SAP to provide XBRL tools in their software).

¹⁷⁹ <http://edocket.access.gpo.gov/2009/E9-12902.htm>

¹⁸⁰ O'Hara & Gerth, *supra* note ____ (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)

responsible for technological development and implementation within private firms, regulator analyses produce similar analytical failures.

Administrative structures and processes geared towards ameliorating “cognitive” independence, capture and turf problems, therefore, must be part of any restructuring of financial regulators, especially in the development of their systemic risk regulation capacity. These structures might be drawn from successful experiments in other contexts—like the Department of Homeland Security’s “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.¹⁸¹ They can provide the strength of “peer review” from a variety of viewpoints, in an attempt to pierce the opacity of risk management technology choices, and the type of situation faced by financial regulators who ultimately had to rely on “intuition” about the strength of private party risk measurement.¹⁸²

C. *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 vision of regulator capability to develop “rolling best practices” by collecting data from regulated entities about what works and what does not, and then disseminating that information back, through education and capacity building.¹⁸³ 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.¹⁸⁴

¹⁸¹ See DHS Privacy Office, Data Integrity, Privacy, and Interoperability Advisory Committee, 69 FED. REG. 18,923 (Apr. 9, 2004); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 104-05 (2008) (discussing the role of the Board in DHS’s compliance with the Privacy Impact Assessment requirements of the EGovernment Act).

¹⁸² See Geithner NY Fed 2006 report.

¹⁸³ Dorf & Sabel, *supra* note __, at 350.

¹⁸⁴ See Bamberger, *Regulation as Delegation*, *supra* note __, at 465 (pointing to the regulatory model settlement agreements, which “are characterized not just by cooperation, but by cooperation ‘in the shadow’ of enforcement”).

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 both firms and GRC developers on how best to comply with privacy regulations.¹⁸⁵ 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.¹⁸⁶ The FTC then made the transcripts of the 2003 workshop panels available through their website, and has also made videotapes of the sessions available.¹⁸⁷

Enhancing the Ex Ante Approval Lever

Second, financial regulators might, again taking cues from the FDA, engage in forms of “approval regulation,”¹⁸⁸ by which individual financial institutions or technology providers would provide full transparency regarding proposed risk-management technologies *ex ante*, and agree to greater disclosure throughout, 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 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.

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 on which management-based

¹⁸⁵ See FTC website at <http://www.ftc.gov/bcp/workshops/technology/index.shtm>.

¹⁸⁶ See Federal Register notice of the public workshops, available at <http://www.ftc.gov/os/2003/02/techwrkshpsfrn.htm>.

¹⁸⁷ See FTC website at <http://www.ftc.gov/bcp/workshops/technology/index.shtm>.

¹⁸⁸ See Daniel Carpenter, *Approval Regulation*.

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' relative risk-management success rests both on the fact that their technology flagged anomalous loss trends, but also 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 trader 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."¹⁸⁹ Specifically, Sarbanes-Oxley's certification requirements provide for what might be called "attention regulation,"¹⁹⁰ 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,"¹⁹¹ and might be employed by forcing other individuals to focus attention on specific red flags through requirements of reporting 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 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

189. Cynthia A. Glassman, Comm'r, SEC, Speech by SEC Commissioner: Remarks at the Practicing Law Institute—SEC Speaks (Feb. 28, 2003), <http://www.sec.gov/news/speech/spch022803cag.htm> (last visited Sept. 8, 2006).

¹⁹⁰ Bamberger, *Regulation as Delegation*, *supra*, note __, at 386.

¹⁹¹ Mark Jensen, Panel Presentation, Conference on Post-Enron Corporate Regulation: Has the Pendulum Swung Too Far (or Not Far Enough)? at the University of California at Berkeley, Boalt Hall School of Law (Mar. 17, 2006) (on file with the author).

explain the decisions taken to regulators and other outside parties—in short to exercise the judgment delegated to them.¹⁹² Such requirements should be triggered both by periodic requirements, and also by individual occurrences, such as by loss events or systemic trends. These processes have, in a variety of contexts in which humans and computer systems interact, increased “social accountability” of decisionmakers.¹⁹³ 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.¹⁹⁴ This, in turn, reduces instances of automation bias through decreased errors of omission and commission, and improves overall task performance.¹⁹⁵ By these means, technology can better be cabined to the role of decision support, rather than decision-maker.

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 policymaking, as well as particular policy choices. Regulators acutely aware of technological limitations on the ability to develop real-time analysis, or on the analytic ability to 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 the choices of 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 suggests a new approach towards precaution in regulation.

¹⁹² See Murray G. Millar & Abraham Tesser, *Thought-Induced Attitude Change: The Effects of Schema Structure and Commitment*, 51 J. PERSONALITY & SOC. PSYCHOL. 259 (1986); Angelo C. Valenti & Abraham Tesser, *On the Mechanism of Thought-Induced Attitude Change*, 9 SOC. BEHAV. & PERSONALITY 17 (1981).

¹⁹³ L.J. Skitka, *et al.*, *Accountability and Automation Bias*, 52 INT'L J. HUMAN-COMPUTER STUD., 701 (2000).

¹⁹⁴ B. Friedman & P. H. Kahn, *Human Agency and Responsible Computing: Implications for Computer System Design*, in B. Friedman (ed.), HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY 221 (1997) (discussing the importance of ensuring that technology systems, like those involved in assessing whether to remove life support, are used as a consultation tool to aid in the decision of removing life support, rather than as a fully “closed loop” decision system).

¹⁹⁵ Skitka, *et al.*, *supra* note ____.

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 and 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 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 consequent ways in which they disable the reasoned judgment of human decisionmakers they inform.¹⁹⁶

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 public 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.”¹⁹⁷ And policymakers must let

¹⁹⁶ See, e.g., Daniel A. Farber, *NEPA and Uncertainty* (draft of April 17, 2009, on file with author) (discussing such problems in the assessment and mitigation of climate change); Douglas A. Kysar, *It Might Have Been: Risk, Precaution, and Opportunity Costs*, Cornell Legal Studies Research Paper No. 06-023 (2006), available at SSRN: <http://ssrn.com/abstract=927995> (discussing such problems in the context of cost-benefit analysis).

¹⁹⁷ Farber, *supra* note __ (describing Daniel Sarewitz et al., *Conclusion, in PREDICTION: SCIENCE, DECISION MAKING, AND THE FUTURE OF NATURE* 359, 369 (2000)).

the fact of imprecision—human or 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.