Governance

Trust, transparency
and smarter business

Our diligent approach to governance — measuring compliance, managing risk and engaging public discourse — enables IBM to innovate while maintaining the trust of clients and society.
Governance at IBM

IBM has a culture based on ethics and integrity, guided by a rigorous system of corporate governance. Grounded in our standards, we remain committed to addressing today’s challenges through transformative leadership, innovation, values and essential partnerships. In this section you’ll find examples of how we continue to enhance the ways we govern our company, manage risk and contribute our expertise to public discourse.

IBM senior management, overseen by our Board of Directors, is responsible for the company’s economic, environmental and social performance, as well as for adherence to IBM’s overall compliance programs. Corporate responsibility is integrated across the business through the following forums.

Corporate Responsibility Executive Steering Committee
Chaired by the vice president for Corporate Citizenship, our Corporate Responsibility Executive Steering Committee provides leadership and direction on key corporate responsibility issues. The committee comprises senior executives from functional areas across the company, with each area responsible for developing its own corporate responsibility goals and strategy. Organization-wide goals are approved by the steering committee.

Corporate Responsibility Working Group
The Corporate Responsibility Working Group manages IBM’s corporate responsibility activities and stakeholder engagement. Meeting at least monthly to review key policy and strategic issues and make recommendations to the steering committee, the working group consists of representatives from 10 functional areas across the company, including global representation. Daily activities are coordinated in the Corporate Citizenship organization, which reports to the chief communications officer.

Ethics and integrity leadership
Creating and maintaining IBM’s sustained culture of ethics and integrity starts with our employees and leaders and extends to our business partners and suppliers. We teach, listen and collaborate, as we continue to transform and enhance our internal compliance, education and integrity programs.

Teach: IBM achieved 100 percent participation in its Business Conduct Guidelines (BCG) program—employees around the world certified our BCG policy, currently available in 25 languages, and completed the BCG course. The BCG course includes an introductory video from our Chairman emphasizing the importance of integrity to IBM and business scenarios depicting integrity decisions that employees may face while conducting IBM’s business.

IBM’s trust and compliance (T&C) officers, lawyers and management in 2017 provided in-person compliance and ethics training to more than 26,000 IBMers around the world on topics including public procurement, business amenities, anticorruption and ethics. Additionally, more than 28,000 IBMers completed Corporate T&C University online education lectures. For employees facing new integrity challenges at turning points in their careers—for example, when they are new to IBM, new to management or new to emerging markets—targeted integrity training is required.

Also in 2017, IBM senior business leaders around the world sponsored integrity summits in 34 countries, in both emerging and major markets. These summits, managed and run by local senior leadership, emphasized the role of leaders in creating an ethical culture and focused on key compliance risks in each region, along with specific actions that can be taken to mitigate these risks.

Listen: For more than 50 years, IBM has maintained an internal “speak up” reporting channel for employees, as well as channels for suppliers, business partners and others to report concerns or suspected violations of our BCGs or unethical or unlawful behavior to the company. These channels support anonymous reporting.

In 2017, nearly 24,000 IBMers completed our annual Global Integrity survey, providing valuable feedback on their perception of ethics and integrity within the organization. We use the insights...
gathered from these annual surveys, completed since 2010, to enhance our global ethics and integrity programs.

Collaborate: IBM's commitment to ethics and integrity leadership extends to our IBM Business Partners' and suppliers' employees, as part of their partnership commitment to IBM. In 2017, IBM provided online ethics and integrity education to more than 15,000 representatives from our IBM Business Partners and suppliers around the world. IBM Business Partner and supplier personnel have received in-person training in connection with our integrity summits in some emerging markets. For the fifth year in a row, IBM’s chief trust and compliance officer emphasized the value of ethics and integrity in an annual address at our Global Business Partner Leadership Conference (PartnerWorld®).

Security and privacy

Responsible data stewardship is central to IBM's commitment to its clients. This approach is surprisingly unusual within the tech industry today, but it is how IBM has always done business. As a result, data privacy and security have been, and will continue to be, a critical consideration for all aspects of our business.

IT security

As companies continue to expand their businesses and IT infrastructure — adding more devices and increasing connectivity — their vulnerabilities can also increase. At IBM, we not only carefully consider security when developing our technology solutions, but also examine our internal systems and processes to assess how we can best reduce risk and maintain the continuity of our business.

The human element also puts businesses at risk as attackers take advantage of lapses in security or use social engineering to target unwitting users. Recognizing that education is among the best forms of protection, we continuously strive to reinforce a cybersecurity-aware culture within our company and throughout the communities around us, by promoting increased knowledge and understanding of relevant issues. Because threats continuously evolve, each of IBM’s employees is required to complete an annual cybersecurity and privacy course that is regularly updated with new insights on the latest types of attacks and security best practices.

Embracing regulatory change

IBM has been at the vanguard of rapidly evolving data privacy regulations. We were one of the first companies to appoint a chief privacy officer, to develop and publish a genetics privacy policy, to be certified under the APEC Cross-Border Privacy Rules system, and to sign the EU Data Protection Code of Conduct for Cloud Service Providers (the EU Cloud Code of Conduct). IBM is bringing that same spirit to implementation of the EU General Data Protection Regulation (GDPR).

Effective May 25, 2018, the GDPR represents the biggest change in data privacy legislation in two decades. IBM has established and is executing a global program to prepare our internal processes and our commercial offerings for the GDPR. As part of this program, we are enhancing our ongoing commitment to “privacy by design,” to help ensure that personal data use is limited by default to what is specifically required. We are revising all agreements with our suppliers, vendors and clients where personal data is collected or processed, and incorporating measures into new and existing contracts to cover the new GDPR requirements. IBM also is leveraging the capabilities of its readiness program to help clients prepare for the GDPR. For more, read about IBM’s Journey to GDPR Readiness, including the IBM GDPR Framework.

Data privacy and security have been, and will continue to be, a critical consideration for all aspects of our business.
Forging industry standards
IBM does not simply wait for regulatory requirements; we actively work within the technology industry to establish prudent standards to safeguard customer data. In 2017, we expanded our participation in the EU Cloud Code of Conduct to cover 24 additional services—making IBM the first company to offer our customers this transparent, independent endorsement across such a large portfolio of services, covering not just infrastructure but also software and platform cloud services. More details are available in this blog post by IBM Chief Privacy Officer Cristina Cabella.

IBM also has certified more than 160 offerings to date for compliance with Privacy Shield; and, in 2017, IBM further certified to the Swiss-U.S. Privacy Shield framework. IBM will continue to certify additional offerings under available frameworks on an ongoing basis.

Fighting to protect customer data
When necessary, IBM will fight to protect customer data under applicable legal frameworks. In 2017, IBM joined a handful of technology companies in supporting a legal challenge to a government request for customer data which, in IBM’s view, did not follow proper channels and process. For more, read the statement by IBM General Counsel Michelle H. Browdy about IBM’s amicus curiae brief to the U.S. Supreme Court. This brief detailed IBM’s long-standing position that government efforts to obtain data for law enforcement purposes should go through recognized legal channels. IBM remains committed to being a responsible participant in the important discussion concerning law enforcement access to data, as well as a strong advocate for our clients.

Enterprise risk management
IBM has developed a consistent, systemic and integrated approach to risk management to help determine how best to identify, manage and mitigate significant risks throughout the company. The IBM Risk Management Framework aligns to industry standards and good practices, focusing on leadership, programs and practices, enablement and effectiveness supported by a strong risk-aware culture.

Leadership and governance
In 2017, the leadership team, compromised of senior management, continued its collaborative process of identifying, evaluating and managing
IBM is focused on applying technology, tools and analytics to support risk management.

Enterprise-level risks. This includes periodic reviews and interaction with the Board of Directors, whose Audit Committee oversees the company’s enterprise risk management (ERM) framework, program and associated processes. Through our executive compensation program, we motivate our leaders to deliver a high degree of business performance without encouraging excessive risk-taking.

Our ERM Executive Council, comprising 17 senior managers representing different units, functions and geographies, meets regularly to help improve the management of enterprise risks. In 2017, we refreshed the ERM Council with seven members rotating off and seven new members replacing them, and we expanded the council for the IBM Credit business. To foster collaboration and transparency, participants share risks and mitigating actions so that the council can more effectively manage risk across the entire enterprise, identifying best practices from one part of the business to standardize and apply across units globally.

Addressing emerging risks
Our company-wide approach to identifying and managing risk is based on the ISO 31000 Risk Management and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM guidance. In adapting these, IBM considers and assesses potential strategic, financial, operational, regulatory and other risks to our business, which could be driven by various factors, such as changes in the external environment, the company’s strategic imperatives and where and how we do business.

Over the course of the year we held in-depth discussions with leading consultants on emerging risks and conducted a robust internal study that included polling, surveys and interviews of approximately 150 top executives. In 2017, we held a design thinking session with leaders from IBM Research to identify emerging risks and trends. As a result, we updated our enterprise-level risk map and refined senior management focus for 2018.

Advancing risk management through analytics and cognitive
IBM is focused on applying technology, tools and analytics to support risk management. In 2017, we continued to build upon the success of the award-winning Country Financial Risk Scorecard; we enhanced the predictive algorithms, expanded coverage and performed deep dive assessments of the risk environment across several countries. Analytics and cognition are the next big frontiers for risk management which, when coupled with the abundance of data, provide the ability to infuse insight into risk management. In 2017, we deployed to over 100 countries our cognitive-based tool to automate the identification of emerging storylines and risks and project possible future scenarios and implications. The tool enhances our global geographic leaders’ risk awareness and ability to improve local resiliency to risks.

Benchmarking and effectiveness
An effective risk management framework should ultimately lead to improved business performance and help the company protect its reputation while delivering on its social responsibilities. IBM continuously evaluates its ERM practices for effectiveness and alignment with those priorities. In 2017, we established and baselined a set of new enterprise-level metrics for effectiveness. We also continued to collaborate with Internal Audit, Trust and Compliance, Business Controls and other oversight organizations to enhance IBM’s approach to identifying, prioritizing and addressing risk within business processes, in order to improve support for risk-based controls and assurance. Lastly, we continued our benchmarking with other leading organizations to provide insights to good practice and emerging risks.

Driving a risk-aware culture
The success of the framework is predicated on a strong culture of risk awareness, identification, analysis and mitigation. To support this, IBM continued to deploy education modules in video formats and provide awareness and transparency through global video blogs, case studies, external perspectives and business leader risk and tool training. In 2017, approximately 50,000 IBMers from around the world collaborated in internal social communities, engaging with a range of materials and risk-management experts, to broaden their risk education.
Advancement through community engagement
Community engagement helps advance the risk management acumen of our current and future business leaders. In 2017, we participated on five ERM councils, including advisory board membership for two university ERM programs, and delivered presentations on contemporary risk best practices at IBM- and non-IBM sponsored industry events.

Principles for trust and transparency
IBM believes organizations that collect, store, manage or process data have an obligation to handle it responsibly. That belief—embodied in our century-long commitment to trust and responsibility in all relationships—is why the world’s largest enterprises trust IBM as a steward of their most valuable data.

In October 2017, IBM Chairman Ginni Rometty told the Financial Times, “We’re entering an era in which data can be used to solve all sorts of the most pressing problems, but only if there’s trust in how that data has been handled.” We take that trust seriously, and in 2017 launched a comprehensive statement of beliefs and practices that we follow in advancing new technologies and growing the digital economy.

We expanded on that in May 2018 with three “principles for trust and transparency” for protecting client data and insights, and for providing the responsible, transparent use of AI and other transformative innovations. They include:

The purpose of AI is to augment human intelligence.
The purpose of AI and cognitive systems developed and applied by IBM is to augment—not replace—human intelligence. Our technology is and will be designed to enhance and extend human capability and potential. At IBM, we believe that AI should make all of us better at our jobs, and that the benefits of the AI era should touch the many, not just the elite few. To that end, we are investing in initiatives to help the global workforce gain the skills needed to work in partnership with these technologies.

Data and insights belong to their creator.
IBM clients’ data is their data, and their insights are their insights. Client data and the insights produced on IBM’s cloud, or from IBM’s AI, are owned by IBM’s clients. We believe that government data policies should be fair and equitable and prioritize openness.

– Data ownership: Clients are not required to relinquish rights to their data—or insights derived from it—to have the benefits of IBM’s solutions and services.
– Data privacy: IBM is fully committed to protecting the privacy of our clients’ data, which is fundamental in a data-driven society.
– Data security: IBM is devoting our powerful engines of innovation to create tools to protect our clients, their data and global trade from cyberthreats, and convening a broader discussion on balancing security, privacy and freedom.
– Government access to data: IBM has not provided client data to any government agency under any surveillance program involving bulk collection of content or metadata.
– Cross-border data flows: IBM views the free movement of data across borders as essential to 21st-century commerce.

New technology, including AI systems, must be transparent and explainable.
For the public to trust AI, it must be transparent. Technology companies must be clear about who trains their AI systems, what data was used in that training and, most importantly, what went into their algorithm’s recommendations. If we are to use AI to help make important decisions, it must be explainable. IBM will make clear:

– When and for what purposes AI is being applied.
– The major sources of data and expertise—and the methods—used to train AI systems and solutions.
– Although bias can never be fully eliminated, IBM and all companies advancing AI have an obligation to address it proactively. We therefore continually test our systems and find new data sets to better align their output with human values and expectations.

Learn more at ibmpolicy.com/trust-principles.