

Sección Internacional

Cumplimiento como Gobernanza: Cognición Organizacional, Riesgo y la Transformación de la Toma de Decisiones Institucional

Entrevista a Larry Catá Backer

Por: Juan Pablo Sarmiento Erazo.

Larry Catá Backer

Es W. Richard and Mary Eshelman Faculty Scholar Professor of Law and International Affairs en la Universidad Estatal de Pensilvania (Pennsylvania State University) y miembro fundador de la Coalition for Peace & Ethics. Su investigación y docencia se concentran en los campos del derecho constitucional, el derecho corporativo y el derecho transnacional. Entre los cursos que imparte se encuentran Responsabilidad Social Corporativa, Derecho y Política de las Empresas Multinacionales, Actores, Instituciones y Marcos Jurídicos en los Asuntos Internacionales, así como asignaturas de derecho constitucional, derecho corporativo y teoría del derecho. Ha presentado sus investigaciones en distintos países sobre temas como la globalización, la inversión soberana, la producción global —incluida la Iniciativa de la Franja y la Ruta (Belt and Road Initiative)—, las empresas y los derechos humanos, el constitucionalismo comparado y los sistemas marxista-leninistas de China y Cuba. Sus investigaciones más recientes abordan la regulación de las empresas multinacionales, el constitucionalismo transnacional y teocrático, la gobernanza basada en datos —incluidos los sistemas de crédito social en China— y la arquitectura internacional para la regulación de las empresas y los derechos humanos. Es miembro electo del American Law Institute y editor de la colección Globalization Law & Policy Series de la editorial Routledge. Áreas de especialización: derecho corporativo comparado y estadounidense, globalización, derecho constitucional, y derecho y política transnacionales.

Resumen

A través de la indagación sobre la internalización de la cultura de cumplimiento, la gestión del riesgo en el sector público, la eficiencia operacional, la inteligencia artificial y la tecnología regulatoria *(RegTech)*, la convergencia entre el cumplimiento y los criterios ESG, la integración de sistemas de gestión fragmentados y las dimensiones reputacionales de la debida diligencia, este análisis despliega el concepto de *gramáticas de gobernanza:* aquellos vocabularios interconectados pero diferenciados —cumplimiento, riesgo, ESG, debida diligencia en derechos humanos, *RegTech*— mediante los cuales las instituciones observan, interpretan y actúan sobre entornos normativos superpuestos y con frecuencia contradictorios. Sustentado en la teoría de sistemas, la semiótica jurídica y la práctica investigativa sobre gobernanza transnacional, el trabajo sostiene que el rasgo distintivo de un cumplimiento maduro no estriba en la densidad de las reglas ni en la sofisticación técnica del monitoreo, sino en la capacidad institucional para traducir la información en decisiones responsables a través de fronteras organizativas y computacionales. Se presta especial atención a la transformación introducida por la inteligencia artificial y la gobernanza guiada por datos, la cual desplaza el riesgo de ser una categoría discreta y transaccional para convertirlo en una propiedad emergente y en continua evolución de los sistemas organizacionales, exigiendo repensar de modo correlativo la apetencia al riesgo, el juicio institucional y la rendición de cuentas a medida que la gobernanza misma se torna crecientemente computacional.

Marco Conceptual

Larry Catá Backer desarrolla en este Marco Conceptual una aproximación al debate contemporáneo sobre el cumplimiento y su transformación en el ámbito de la gobernanza organizacional, examinando los nuevos desafíos regulatorios, tecnológicos y de sostenibilidad que inciden en las organizaciones.

El debate contemporáneo sobre el cumplimiento refleja, de manera cada vez más evidente, una transformación estructural en la naturaleza de la gobernanza organizacional. Si bien el cumplimiento surgió históricamente como un dispositivo para garantizar el acatamiento de deberes legales y exigencias regulatorias, su cometido actual se ha expandido de modo considerable. Las organizaciones se desenvuelven hoy dentro de entornos complejos signados por expectativas normativas múltiples y superpuestas, que abarcan desde la regulación interna y las normas internacionales hasta los compromisos contractuales, los estándares de sostenibilidad, la responsabilidad en materia de derechos humanos, los requerimientos de los inversionistas, los sistemas tecnológicos y la escrutadora mirada de los diversos actores interesados.

En este contexto, el cumplimiento no puede reducirse a un mecanismo defensivo orientado a evitar infracciones. Opera, de forma creciente, como una arquitectura institucional a través de la cual la organización identifica información relevante, interpreta expectativas en conflicto, asigna responsabilidades, estructura sus procesos decisionales y se adapta de manera continua a circunstancias cambiantes.

Esta transformación no implica que el cumplimiento legal tradicional haya desaparecido; las normas, los deberes, las medidas de ejecución y la supervisión regulatoria continúan siendo ejes articuladores de la gobernanza. Ocurre, más bien, que el cumplimiento contemporáneo se despliega simultáneamente a través de diversas modalidades complementarias de razonamiento institucional. Los enfoques basados en reglas resultan indispensables allí donde se requiere trazar límites jurídicos precisos; los enfoques basados en el riesgo auxilian a la organización a encauzar la atención y los recursos en condiciones de incertidumbre; los marcos de ESG, sostenibilidad y debida diligencia en derechos humanos amplían la mirada hacia los impactos, las relaciones y la legitimidad de largo plazo; y las tecnologías regulatorias *(RegTech)* junto a la inteligencia artificial transforman radicalmente la celeridad, la escala y los métodos mediante los cuales la institución observa y procesa la información.

Estas aproximaciones no deben interpretarse necesariamente como etapas secuenciales por las que la organización deba transitar de modo inevitable. Tales narrativas constituyen simplificaciones analíticas útiles, pero corren el riesgo de eclipsar el hecho de que las instituciones emplean con frecuencia múltiples enfoques de manera simultánea. Una empresa multinacional puede articular, al mismo tiempo, controles jurídicos formales, analítica de riesgos, evaluaciones de sostenibilidad, debida diligencia en derechos humanos y monitoreo computacional. La cuestión determinante no estriba, por ende, en qué modelo desplaza a otro, sino en cómo interactúan estas distintas modalidades dentro de la organización.

Dicha articulación se comprende mediante el concepto de *gramáticas de gobernanza*, del

cual considero tres variaciones. La primera es la *gramática sistémica*, orientada a cómo se manifiesta el asunto una vez que la organización se concibe como un sistema comunicativo recursivo. La segunda es la *gramática de gobernanza*, centrada en cómo el cumplimiento, los criterios ESG, el riesgo, la debida diligencia en derechos humanos, la auditoría y el *RegTech* se convierten en gramáticas diferenciadas y no en meras funciones independientes. La tercera es la *gramática computacional-cuántica*, la cual reviste dos formas: una enfocada en cómo la cognición de la máquina altera la producción de sentido organizacional, y otra que abandona el antropocentrismo de la producción económica para centrarse en los sistemas mismos, dentro de los cuales el ser humano figura como factor u objeto pero no necesariamente como el motor determinante. El eje no reside en la predicción ni en la teoría abstracta, sino en las transformaciones que sobrevienen cuando se deja de presuponer que la gobernanza opera mediante cogniciones secuenciales.

Una gramática rebasa la noción de un mero repertorio léxico; constituye la estructura que torna significativa a la información, determinando cómo se clasifican, conectan, interpretan, comunican y traducen en acción las observaciones. De forma análoga, las organizaciones se apoyan en gramáticas de gobernanza: sistemas conceptuales, procedimentales, indicadores, estándares, esquemas de reporte y procesos decisionales a través de los cuales otorgan sentido a la complejidad del entorno.

El cumplimiento, la gestión del riesgo empresarial, los enfoques ESG, la debida diligencia en derechos humanos, la auditoría interna, la gobernanza de la ciberseguridad y el *RegTech* pueden entenderse, en consecuencia, como gramáticas de gobernanza distintas pero interconectadas, donde cada una acentúa dimensiones específicas de la realidad organizacional. No se trata de compartimentos aislados, sino de modos diversos de observar, interpretar y gobernar una misma dinámica institucional. Podría sugerirse que el cumplimiento enfatiza la conformidad legal y la integridad institucional; la gestión de riesgos se centra en la incertidumbre y la exposición; los enfoques ESG privilegian la sostenibilidad, las expectativas de los grupos de interés y la resiliencia a largo plazo; la debida diligencia en derechos humanos atiende a los impactos en las relaciones organizacionales y cadenas de valor; y el *RegTech* prioriza la observación computacional, el monitoreo y el análisis predictivo.

La incorporación creciente de la inteligencia artificial y de sistemas de datos avanzados introduce una mutación adicional. Históricamente, las instituciones dependían de la observación periódica: auditorías, investigaciones, ciclos de reporte y revisiones directivas. Los sistemas computacionales permiten hoy una observación continua mediante análisis automatizados, reconocimiento de patrones, detección de anomalías y modelado predictivo. Ello no suprime el juicio humano, sino que reconfigura la relación entre dicho juicio y la información institucional.

El desafío central de la gobernanza no radica entonces en la simple posesión de datos, sino en la disponibilidad de sistemas confiables para interpretarlos y convertirlos en decisiones responsables.

Es por esta razón que el cumplimiento contemporáneo concierne de modo creciente a la cognición organizacional. La cuestión decisiva no es solo si la institución conoce las reglas aplicables, sino si posee la capacidad para observar condiciones cambiantes, interpretar riesgos emergentes, comunicarse a través de sus fronteras internas y adaptarse antes de que el daño se concrete.

Las respuestas que siguen examinan el cumplimiento bajo este horizonte amplio, abordando cada interrogante primero como un problema práctico de gobernanza para luego analizarlo a la luz de las transformaciones institucionales, sistémicas y computacionales que moldean a las organizaciones contemporáneas.

1. A nivel internacional se debate el paso de un cumplimiento reactivo hacia un modelo basado en la cultura organizacional. Desde su experiencia, ¿qué indicadores o señales concretas demuestran que un programa ha sido verdaderamente internalizado y no permanece como un mero "cumplimiento cosmético"? ¿Podría compartir métricas o ejemplos prácticos que haya constatado como particularmente eficaces?

R/. Un punto de partida útil, en consonancia con el tránsito de la regulación de mando y control hacia sistemas de autoconstitución y normatividad interna en la literatura académica de gobernanza transnacional, consiste en diferenciar entre el cumplimiento entendido como una restricción externa impuesta a la organización y el cumplimiento concebido como una lógica operativa interna que la institución ha absorbido en la arquitectura de sus propias decisiones. Lo primero genera lo que la práctica denomina con acierto "cumplimiento cosmético": políticas que existen en el papel y satisfacen el inventario de un auditor, pero que no guían la conducta real. Lo segundo da lugar a algo más cercano a un sistema estructuralmente acoplado, donde las normas de cumplimiento forman parte de la manera en que la institución percibe el riesgo, asigna recursos y evalúa a su personal, en lugar de constituir una capa superpuesta sobre una lógica de negocios preexistente. La distinción entre cumplimiento cosmético e internalizado se reduce, en última instancia, a la diferencia entre una exigencia organizacional externa y un componente intrínseco de la arquitectura decisional.

Un programa se mantiene en el plano de lo cosmético cuando su función principal es la demostración simbólica de conformidad. En tales escenarios, la organización puede exhibir códigos de conducta, programas de capacitación, certificaciones y canales de denuncia, pero tales instrumentos operan primordialmente como representaciones hacia afuera más que como mecanismos que modelen el comportamiento interno.

El cumplimiento internalizado revela otra naturaleza, haciéndose perceptible cuando las consideraciones normativas ingresan en los procesos ordinarios de toma de decisiones antes de que irrumpan los problemas. La cuestión no estriba en poseer documentos de cumplimiento —prácticamente toda organización de envergadura los tiene—, sino en determinar si esos documentos, procedimientos y arreglos institucionales influyen efectivamente en la toma de decisiones.

Es posible esbozar ciertos indicadores concretos que sugieren la presencia de una internalización real frente a la mera adopción formal.

Sobresale, en primer término, la conducta de escalamiento orientada hacia protocolos de prevención y mitigación. Una organización con un cumplimiento internalizado muestra una dinámica saludable en la que los problemas se plantean antes de volverse críticos, alcanzando a las instancias de cumplimiento los incidentes menores, los escenarios hipotéticos y las dudas de los empleados de nivel medio sin temor a represalias. Un programa que produce reportes únicamente cuando los reguladores o auditores indagan continúa siendo reactivo. Ahora bien, las conductas de escalamiento no se agotan en la vertiente vertical dentro de los departamentos; poseen también una dimensión horizontal decisiva. La información sobre cumplimiento debe circular por la organización en lugar de permanecer concentrada en una dependencia especializada. Cuando las unidades de negocio, los equipos de compras, los responsables financieros, los gerentes operativos y la alta dirección incorporan sistemáticamente estas consideraciones en su planeación, el cumplimiento deja de ser un control externo para convertirse en una función de gobernanza interna.

Destaca asimismo la integración de la expectativa de priorizar la prevención y la mitigación por encima de la remediación. Siguiendo el modelo de expectativas de los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos para estructurar la conducta empresarial, la toma de decisiones y la evaluación de riesgos —como elemento medular del cumplimiento— se orientan a situar en primer plano la prevención y la mitigación. Esta mutación implica concebir el cumplimiento con carácter prospectivo y no retrospectivo. El cumplimiento tradicional se ha centrado con frecuencia en identificar infracciones tras su ocurrencia; una arquitectura madura procura identificar previamente las condiciones que hacen más o menos factibles tales infracciones, lo cual exige integrar estas consideraciones en la estrategia, la contratación, la gestión de la cadena de suministro, las adquisiciones, las inversiones y la planificación operativa.

Se observa también la ponderación del riesgo mediante matrices de evaluación multifactoriales. Este aspecto resulta acaso más controvertido dentro de la comunidad de derechos humanos y sus aliados políticos o administrativos. Las instituciones que evalúan no solo la ocurrencia de infracciones sino la manera en que responden a la incertidumbre tienden a evidenciar un tránsito del exterior al interior del cumplimiento. Ninguna organización compleja puede erradicar la totalidad de los riesgos; el indicador más significativo estriba en si posee mecanismos para identificar problemas, escalar inquietudes, investigar adecuadamente y aprender institucionalmente de la experiencia en función de sus objetivos clave, las políticas estatales pertinentes, las expectativas del mercado, los planes a corto y largo plazo y, en ciertos casos, la gravedad del impacto y la solidez de los efectos positivos de las decisiones proyectadas.

A ello se suma la asignación de recursos con independencia de los ciclos de fiscalización. La internalización profunda se evidencia cuando los presupuestos, el personal y la capacitación se mantienen o incrementan durante períodos de baja atención regulatoria, es decir, cuando la organización no se limita a reaccionar ante los riesgos de divulgación que desencadenan litigios o procesos administrativos y penales. No se trata solo de reparar a las partes afectadas, sino de asumir las consecuencias derivadas de la potestad civil y penal del Estado, todo lo cual se amplifica cuando una empresa gestiona múltiples órdenes de cumplimiento a lo largo de cadenas transnacionales de suministro.

Cuentan igualmente la integración en la evaluación del desempeño y la compensación —donde la adhesión a las normas de cumplimiento pondera en las promociones y retribuciones de la directiva— y la fluidez conceptual de la junta directiva y la alta gerencia, quienes deben ser capaces de articular la sustancia de los riesgos principales con palabras propias, pues la delegación huérfana de comprensión constituye un rasgo inequívoco de cumplimiento cosmético.

A ello debe añadirse la consistencia en la aplicación de estándares a lo largo de líneas de negocio tanto favorecidas como secundarias. Un cumplimiento internalizado aplica la misma vara a una unidad de altos ingresos que a una marginal; allí donde la sanción es severa para las áreas de bajo rendimiento y laxa para las estrellas, el programa atiende a la apariencia y no a la gobernanza de la conducta.

En términos prácticos, esto se evalúa mediante indicadores longitudinales antes que con auditorías estáticas: líneas de tendencia en incidentes autoinformados, métricas de tiempo de escalamiento, encuestas de clima sobre la seguridad psicológica para expresar inquietudes y, de modo fundamental, la constatación de si los hallazgos de cumplimiento han alterado alguna vez una decisión comercial estratégica. Una entidad que pueda señalar al menos un caso en que las consideraciones de cumplimiento se impusieron sobre una oportunidad rentable ofrece una prueba empírica de internalización que ningún documento de política puede suplantar.

Con todo, este marco sugiere también que la madurez en el cumplimiento no se mide ex-

clusivamente por métricas de resultado. Una empresa con pocas infracciones reportadas puede contar sencillamente con sistemas de detección deficientes; a la inversa, una entidad con canales efectivos identificará un número mayor de problemas porque sus empleados confían en la estructura.

Atendiendo a lo expuesto, los indicadores más reveladores comprenden: (1) el grado en que las consideraciones de cumplimiento se integran en las decisiones de negocio; (2) la celeridad y calidad de los procesos de escalamiento interno; (3) la capacidad de transformar los hallazgos en aprendizaje organizacional; (4) la alineación de los incentivos con los objetivos de cumplimiento; (5) la disposición de la alta gerencia a tratar la información de cumplimiento como insumo decisional y no meramente regulatorio; y (6) la efectividad con que las distintas unidades comparten la información sobre riesgos.

Tales indicadores revelan aspectos esenciales sobre la cultura organizacional y las expectativas socioeconómicas del entorno empresarial, tanto en el ámbito jurídico como en los mercados. Conviene enfatizar que la cultura de negocios —entendida como la suma de estas expectativas y las estructuras para su aplicación racional— no debe concebirse primordialmente como un conjunto de creencias individuales. Las organizaciones no poseen una conciencia análoga a la humana; su cultura se manifiesta a través de patrones reiterados de comunicación, toma de decisiones, incentivos y memoria institucional. Es en este sentido semiótico y computacional —asentado en un proceso inductivo a partir de la agregación de iteraciones decisionales y de comportamiento (datos operacionales relevantes)— que la cultura empresarial puede comprenderse y medirse consigo misma por referencia al ideal que la agregación representa en su sector, o frente a un ideal exógeno. Esta segunda modalidad, la medición frente a un ideal externo, define con precisión la relación entre el Estado y las empresas en el marco de la actividad económica de mercado. Introduce el impulso deductivo y configura la dialéctica medular del cumplimiento como una tensión entre el proceso inductivo de formación cultural de las empresas "a través del actuar" (fenomenología inductiva) y el proceso de dirigir, encauzar y disciplinar dicha formación frente a las desviaciones mediante medidas regulatorias y de supervisión organizadas desde los órganos estatales (la arquitectura deductiva de la integridad institucional colectiva).

El fenómeno puede apreciarse con distintos matices según el prisma que se adopte. Desde la perspectiva sistémica, el cumplimiento internalizado ocurre cuando este se integra en la estructura comunicativa ordinaria de la institución. Desde la perspectiva de las gramáticas de gobernanza, la internalización se alcanza cuando el lenguaje del cumplimiento se convierte en una de las lenguas habituales mediante las cuales la organización interpreta sus opciones, sin requerir una evaluación posterior a los hechos, sino integrándose en la gestación misma de las decisiones hasta diluirse en la cultura organizacional como una de sus premisas ordenadoras.

Formulado en los términos del esquema tripartito introducido al inicio, la internalización constituye ante todo un fenómeno de *gramática sistémica*: el cumplimiento se vuelve parte de las operaciones comunicativas ordinarias de la organización y no un insumo externo procesado por un departamento especializado. Alcanza su madurez de *gramática de gobernanza* cuando funciona como una lengua de trabajo para construir decisiones, y no para juzgarlas a posteriori. Finalmente, adquiere una dimensión *computacional-cuántica* cuando la observación de la máquina se suma a la cognición organizacional, desarrollo que abordamos más adelante. Para un oficial de cumplimiento, la consecuencia práctica es directa: la internalización se diagnostica examinando la comunicación (¿surgen las conversaciones sobre riesgo en el vocabulario del cumplimiento, de forma espontánea, en las reuniones ordinarias de negocio?), verificando la arquitectura decisional (¿se sitúa el cumplimiento dentro de la decisión o llega tras ella?) y evaluando si los sistemas de monitoreo computacional y los decisores humanos

se nutren de la misma información o marchan por rieles desconectados.

La inteligencia artificial y el *RegTech* inciden de modo creciente en este proceso al alterar la escala y la velocidad de la observación institucional. Si históricamente el cumplimiento dependía de revisiones periódicas y de la identificación humana de los problemas, las instituciones pueden emplear hoy sistemas computacionales para identificar patrones, detectar anomalías, supervisar transacciones, analizar comunicaciones y prever riesgos emergentes.

Sin embargo, la tecnología por sí sola no genera un cumplimiento internalizado. Un sistema de monitoreo sofisticado puede coexistir con una gobernanza débil si la información producida es ignorada o permanece desconectada de la toma de decisiones. La interrogante decisiva sigue siendo de carácter institucional: ¿dispone la organización de mecanismos para convertir las observaciones en decisiones responsables? Los sistemas de cumplimiento más sólidos no son necesariamente los que acumulan mayor número de controles, sino los capaces de traducir continuamente la información en acción responsable. La métrica definitiva es la autocorrección organizacional: una institución demuestra un cumplimiento genuino cuando detecta, interpreta y corrige sus desviaciones antes de que intervengan los reguladores externos.

2. En muchos países, especialmente aquellos con una marcada tradición de derecho administrativo, la implementación de estándares de cumplimiento en el sector público se percibe a menudo como una carga burocrática adicional. Desde su experiencia internacional, ¿cómo pueden adaptarse los modelos de gestión de riesgos para mejorar de manera genuina la eficiencia y la transparencia, particularmente en áreas sensibles como la contratación pública?

R/. La percepción del cumplimiento como un lastre burocrático constituye a menudo, en tradiciones de derecho administrativo erigidas sobre la legalidad formal y la regularidad procedimental, un síntoma derivado de importar modelos de riesgo del sector privado sin adaptarlos a las exigencias de legitimidad propias de la administración pública. La contratación pública resulta ilustrativa: el impulso del sector privado busca minimizar la fricción transaccional, mientras que la administración pública debe satisfacer requerimientos de igualdad de acceso, revisabilidad y rendición de cuentas que carecen de análogo privado. La idea de que el cumplimiento engendra burocracia nace con frecuencia de una concepción reduccionista de su cometido: si se le entiende como la mera multiplicación de trámites, visados, requisitos documentales y obligaciones de reporte, se le percibirá como una capa administrativa superpuesta a sistemas estatales de por sí complejos.

Una concepción distinta conduce, no obstante, a una conclusión opuesta.

La función medular de la gestión de riesgos no consiste en crear trámites adicionales, sino en elevar la calidad de la observación institucional y de la toma de decisiones en condiciones de incertidumbre.

Esta distinción adquiere particular relieve en la administración pública. Los gobiernos operan en entornos de alta complejidad, caracterizados por la multiplicidad de actores, la cuantía de los recursos financieros, las expectativas políticas, las obligaciones de rendición de cuentas y los horizontes temporales de largo alcance. El desafío no radica en sumar más reglas —las instituciones públicas ya actúan dentro de marcos

legales exhaustivos—, sino en determinar si tales instituciones poseen mecanismos eficaces para identificar, priorizar y responder al riesgo.

Los modelos de gestión de riesgos contribuyen a la eficiencia del sector público cuando desplazan la atención administrativa desde un control procedimental uniforme hacia una observación diferenciada y una respuesta proporcional. Un modelo puramente procedimental indaga si se cumplieron todos los pasos formales; un modelo basado en el riesgo cuestiona en qué áreas resulta indispensable la atención institucional y qué información se requiere para fundamentar esa determinación.

La diferencia es sustancial. El primer enfoque se agota en el proceso, siendo susceptible de la manipulación de incentivos (*reward hacking*, entendido como los atajos no deseados para maximizar señales de recompensa en la programación de máquinas o en las medidas de cumplimiento humano sin completar la tarea de fondo). El segundo contextualiza el proceso dentro de las expectativas y restricciones normativas, permitiendo que los sistemas incorporen precisión y detonantes basados en objetivos mediante el lenguaje y la capacidad computacional del riesgo (identificación, valoración, evaluación y mecanismos de respuesta).

Ciertamente, la adaptación fructífera exige replantear la gestión de riesgos no como un nivel adicional de control sobre los procesos de contratación, sino como un sustituto de formas de control menos eficientes y más discrecionales sobre las que suele descansar el derecho administrativo, tales como las autorizaciones previas exhaustivas, las firmas escalonadas y los litigios ex post. Un modelo de riesgo adecuadamente diseñado puede reemplazar el escrutinio uniforme de cada transacción por una fiscalización diferenciada y calibrada según indicadores reales de riesgo (cuantía del contrato, condición de oferente único, historial del contratista o vulnerabilidades de corrupción sectoriales). Ello no constituye una desregulación, sino la reasignación de la atención regulatoria hacia las operaciones que más la requieren, lo cual incrementa tanto la eficiencia —al agilizar las compras rutinarias de bajo riesgo— como la transparencia, al hacer explícitos y auditables los criterios que activan una revisión agravada, en lugar de dejarlos al arbitrio de la costumbre burocrática.

Tres elementos resultan determinantes en el contexto del sector público:

- La publicación de los propios criterios de riesgo. Cuando los umbrales y las alertas rojas que activan revisiones intensivas son públicos, la contratación se vuelve predecible para los licitadores y menos susceptible a cuestionamientos por arbitrariedad, atendiendo la preocupación central del derecho administrativo respecto a la discrecionalidad.
- Las trazas digitales de auditoría como sustituto de la estratificación procedimental. En lugar de acumular visados secuenciales, la digitalización de los expedientes de contratación permite que cada hito decisional cuente con marca temporal y atribución clara, garantizando una transparencia continua sin paralizar las transacciones en tiempo real.
- La segregación entre las funciones de puntuación de riesgo y las de adjudicación. Mantener la independencia entre la unidad que advierte el riesgo y la que otorga el contrato evita que la gestión de riesgos degenere en una garita discrecional adicional, falla recurrente cuando las funciones de cumplimiento quedan subordinadas a la misma jerarquía que deben fiscalizar.

La contratación pública constituye un ejemplo evidente. Los sistemas tradicionales suelen enfatizar la conformidad formal con los pliegos, los requisitos de habilitación, la documentación y las aprobaciones. Aunque tales resguardos son necesarios, la conformidad formal por sí sola no necesariamente saca a la luz riesgos emergentes como los conflictos de interés, la concentración de proveedores, la colusión, el bajo rendimiento, la vulnerabilidad a la corrupción o las dependencias en la cadena de suministro.

Un sistema de contratación basado en el riesgo complementa la conformidad procedimental con una observación continua. Diseñado adecuadamente, puede traducirse en variables computacionales donde las tecnologías emer-

gentes, en especial los modelos de lenguaje de gran tamaño (LLM) y las redes neuronales, permiten alinear y agilizar los procesos. Tanto en el plano humano como en el computacional, un sistema de esta índole analiza patrones, compara transacciones, detecta anomalías, evalúa relaciones y aprende de los resultados de contrataciones previas. En este sentido, la gestión de riesgos se erige en una arquitectura de información más que en una traba administrativa.

Igual principio aplica a la transparencia y a la rendición de cuentas. La transparencia suele entenderse como mera divulgación de información hacia el exterior; pero aun siendo esta indispensable, la transparencia efectiva requiere capacidad institucional para procesar datos significativos. Una base de datos que albergue millones de contrataciones no genera por sí misma rendición de cuentas: la información debe estructurarse de modo que reguladores, auditores, ciudadanos y decisores puedan interpretarla.

Es en este punto donde la articulación de las gramáticas de gobernanza adquiere relieve. Los distintos actores institucionales observan la contratación pública a través de gramáticas diversas: el responsable de compras atiende a la legalidad procedimental; el funcionario financiero, a la sostenibilidad fiscal; el auditor, a la integridad del control; la sociedad civil, al impacto en el interés público; el analista de derechos humanos, a los riesgos en la cadena de suministro; y el sistema de datos, a las irregularidades estadísticas. La gobernanza efectiva exige la traducción mutua entre estas perspectivas. El objetivo no es anular los distintos enfoques, sino crear mecanismos institucionales mediante los cuales logren comunicarse.

En el léxico del marco tripartito, nos encontramos ante la *gramática de gobernanza* desempeñando su cometido propio: traducir las observaciones procedimentales, fiscales, de auditoría, de la sociedad civil y computacionales sobre una misma decisión de contratación, impidiendo que una sola pretenda usurpar la totalidad. La consecuencia práctica es de índole arquitectónica: una jurisdicción que asuma con seriedad esta función traductora debe contar con un mecanismo específico para ejecutarla —un comité transversal de riesgo con representación permanente de compras, finanzas, auditoría y supervisión independiente, operando bajo una taxonomía pública de riesgo, en lugar de confiar la traducción a coordinaciones informales entre funcionarios que solo dominan su propio lenguaje técnico.

Tradicionalmente, es aquí donde los costos humanos de mantener sistemas efectivos resultan prohibitivos, en el sentido de que el costo de las medidas de cumplimiento supera el valor agregado (neto de los impactos adversos mitigados). Los avances tecnológicos contemporáneos han reducido, o prometen reducir, estos costos humanos sobre actividades económicas cuyo valor no se agota en el cumplimiento, sino en el impacto positivo derivado del empleo óptimo de las fuerzas productivas hacia fines socialmente valiosos (definidos, comprendidos y manifestados contextualmente).

De modo particular, los sistemas de inteligencia artificial y el *RegTech* se han orientado a expandir estas posibilidades. Los sistemas de aprendizaje automático pueden detectar patrones inusuales en miles de licitaciones; el análisis de redes permite vislumbrar vínculos entre proveedores, contratistas e intermediarios; y el procesamiento de lenguaje natural ayuda a examinar cláusulas contractuales para advertir inconsistencias.

Con todo, la capacidad computacional no reemplaza el juicio administrativo. La máquina señala la anomalía; la institución determina su alcance. Una señal computacional deviene en gobernanza únicamente cuando ingresa en un proceso decisional capaz de interpretarla y encauzarla. Por ello, el porvenir del sector público no reside en recortar la administración, sino en organizarla mejor, sirviendo esto como pauta para sistemas más amplios de cumplimiento que requieren el acoplamiento de tecnoburocracias públicas y privadas potenciadas por sistemas de máquinas. La meta no es suprimir estructuras, sino rediseñarlas para encauzar la atención institucional hacia las áreas de mayor relevancia.

Un sistema de cumplimiento maduro no cuestiona cuántos controles pueden imponerse, sino cómo pueden las instituciones públicas desarrollar la capacidad de observar, interpretar y res-

ponder al riesgo con eficacia, y cómo el sujeto regulado puede ser permeado por sistemas de expectativas de conducta internalizados que le permitan ser, de manera creciente, autopolicial. El gran desafío —que desborda el alcance de esta respuesta— radica en la resistencia hacia la arquitectura normativa sobre la que se erigen estos sistemas acoplados. Para quienes consideran que el mercado y la mecánica inductiva constituyen la vía más idónea para generar normas y resolver desafíos, y entienden que las estrategias de prevención, mitigación y remediación deben expresar la experiencia inductiva antes que una conceptualización deductiva hecha carne, el proyecto mismo del cumplimiento puede resultar anómalo y, al ser impuesto, eludido. Ello nos reenvía al cumplimiento cosmético abordado en la Pregunta 1, redefinido ahora como una manifestación de resistencia política y cultural antes que como una simple falla de diseño del sistema, lo cual abre la puerta a la Pregunta 3.

3. El cumplimiento se percibe a menudo como un factor que ralentiza las operaciones comerciales. Sin embargo, en la práctica, también puede generar eficiencias significativas. ¿Cómo puede un programa bien diseñado optimizar los procesos internos y mejorar la toma de decisiones? ¿Ha conocido casos en los que el cumplimiento se haya convertido en una fuente de ventaja competitiva?

La intuición de que el cumplimiento frena la operativa descansa en concebirlo como un control ex post, una garita situada al final del proceso. Cuando las funciones de cumplimiento actúan ex ante, integradas en el diseño mismo de la operación, tienden a reducir el volumen de reprocesos, renegociaciones contractuales y litigios que derivan de decisiones adoptadas sin la debida información de riesgo. En tal sentido, un cumplimiento bien diseñado opera menos como un freno y más como un sistema de navegación: no desacelera el vehículo, sino que evita los desvíos que exigirían desandar el camino.

La fuente más clara de ventaja competitiva surge en mercados caracterizados por una alta densidad regulatoria o reputacional, es decir, aquellos que involucran transacciones transfronterizas, contrapartes reguladas (bancos, compradores públicos, sociedades cotizadas) o cadenas de suministro sujetas a debida diligencia ambiental y de derechos humanos. En estos entornos, la infraestructura de cumplimiento de una contraparte funciona como una señal creíble que reduce los costos de verificación del otro contratante. Un proveedor capaz de acreditar un sistema maduro de trazabilidad y cumplimiento resulta más económico de contratar, no solo más seguro, ya que la contraparte invierte menos recursos en su fiscalización. Es la misma lógica que impulsa la expansión de la debida diligencia en la regulación transnacional: la capacidad de cumplimiento se convierte en un factor de acceso al mercado y no en una simple prevención de riesgos.

Si la idea de que el cumplimiento ralentiza la actividad empresarial refleja una visión reduccionista que lo sitúa como un control externo, cabe examinar cómo una concepción integrada altera esta perspectiva.

El cumplimiento genera eficiencia porque reduce la incertidumbre. Toda institución debe decidir en escenarios de información incompleta. Antes de ingresar a un mercado, adquirir una entidad, seleccionar un proveedor, desarrollar un producto o sellar una alianza, la organización necesita interpretar los datos disponibles y trazar cursos de acción aceptables. Las gobernanzas débiles encarecen la toma de decisiones porque cada paso exige investigaciones, interpretaciones y negociaciones aisladas. Una arquitectura de cumplimiento bien articulada reduce esos costos al fijar marcos decisionales compartidos, entre los que destacan: (1) pro-

cesos estandarizados de debida diligencia; (2) esquemas contractuales consistentes; (3) procedimientos claros de escalamiento; (4) mecanismos confiables de aprobación; y (5) una memoria institucional sobre decisiones previas.

Tales mecanismos no solo previenen conductas indebidas, sino que agilizan la toma de decisiones responsables. Esta fue una de las premisas tutelares de varios de los gestores de los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos. En efecto, parte del trasfondo del Segundo Pilar se basó en la convicción de que una inserción profunda en los procesos empresariales — guiada por la evolución de los principios normativos con que se entiende el riesgo comercial— podía lograrse privatizando el cumplimiento como un sistema autónomo y recursivo, orientado exteriormente por los estándares internacionales de derechos humanos y limitado por lo que los ordenamientos jurídicos estatales lograran articular en su intento (a menudo fallido) de cumplir su deber de protección. La pieza central fue la debida diligencia en derechos humanos, cuyos ecos permean hoy numerosos ordenamientos internos.

Resulta indispensable subrayar la importancia de este aspecto para las empresas multinacionales con presencia en diversas jurisdicciones. A falta de una gobernanza común, cada filial puede desarrollar enfoques dispares ante las obligaciones legales, la evaluación de proveedores, la apreciación del riesgo y el trato con los grupos de interés. El cumplimiento aporta coherencia organizacional al suministrar un lenguaje institucional compartido.

Desde la perspectiva de las gramáticas de gobernanza, el cumplimiento permite que actores distantes geográfica y funcionalmente interpreten situaciones complejas mediante esquemas conceptuales comunes. La ventaja competitiva no surge porque el cumplimiento suprima todas las restricciones, sino porque capacita a la organización para desenvolverse ante ellas con mayor destreza que sus competidores. Una entidad con capacidades maduras de cumplimiento puede vislumbrar desarrollos regulatorios con mayor antelación, evaluar alianzas con superior criterio, incursionar en nuevos mercados con firmeza y reaccionar con celeridad ante los problemas.

Ello se observa con nitidez en la gestión de cadenas de suministro. Las entidades que han consolidado sistemas sólidos de debida diligencia están mejor preparadas para comprender sus redes de proveedores, identificar vulnerabilidades y responder ante interrupciones. La misma regla aplica a las expectativas de sostenibilidad y ESG: las empresas enfrentan crecientes demandas de inversionistas, reguladores y clientes respecto a su desempeño ambiental y social. Mientras que una entidad que aborde estos asuntos como meras obligaciones de reporte externo fatiga en su respuesta, aquella que los ha incorporado en su matriz decisional los utiliza estratégicamente. La relación entre cumplimiento y eficiencia no es contradictoria; depende de si el cumplimiento se gestiona como un trámite de aprobación independiente o como un componente de la inteligencia organizacional.

La transformación computacional refuerza este planteamiento. Los sistemas RegTech pueden aliviar el trabajo administrativo repetitivo, automatizar el monitoreo, elevar la calidad de los datos y suministrar información oportuna a los decisores. Sin embargo, la automatización por sí sola no genera ventaja competitiva; el valor estratégico aflora cuando las herramientas tecnológicas operan dentro de una arquitectura de gobernanza coherente. Las instituciones que más se beneficiarán de sus capacidades de cumplimiento no serán las que acumulen más controles o tecnología, sino las capaces de convertir la información en aprendizaje organizacional. La tecnología aporta la observación; la gobernanza, la interpretación; y la toma de decisiones, la acción. La dimensión semiótica es evidente: la tecnología constituye el objeto-sujeto semiótico (el primer momento); la gobernanza encarna la significación (el segundo momento triádico que otorga carácter sistémico a la cognición humana); y la toma de decisiones representa el tercer momento, la fenomenología de la significación que, mediante la acción, deviene en sentido no solo para el actor, sino como desempeño reforzador del colectivo. La transformación computacional apunta así a un sistema emergente de interacción hombre-máquina

que fluidifica la inserción del cumplimiento no solo en las empresas, sino entre todos los actores de la supervisión. En su punto límite, el ser humano deviene irrelevante para el sistema salvo como su objeto, pasando a ser —en lugar de la tecnología— el primer momento semiótico alrededor del cual el sistema se constituye y el combustible que lo impulsa. Esto nos sitúa en el núcleo de la Pregunta 4.

En los términos del esquema tripartito, este pasaje describe la *gramática computacional-cuántica* operando en su segunda forma, más radical: no ya la cognición de la máquina acelerando las gramáticas existentes, sino un reordenamiento en el que el ser humano deja de ser el centro interpretativo para convertirse en uno de sus insumos. Salvo en ese extremo, la consecuencia práctica es concreta e inmediata: las organizaciones que aspiren a que el cumplimiento sea fuente de eficiencia y no de deriva deben tratar la forma humana no como un formalismo superpuesto al monitoreo automatizado, sino como el espacio donde el segundo y tercer momento semiótico —la significación y la interpretación— continúan siendo ejecutados deliberadamente por una persona responsable, aún cuando el primer momento, la observación subyacente, sea generado de forma creciente por máquinas. Perder de vista esta distinción es el camino por el cual el monitoreo eficiente se transforma en un monitoreo irresponsable.

4. La rápida expansión de la inteligencia artificial y el uso masivo de datos han transformado el panorama de los riesgos legales y éticos. ¿Qué tendencias observa en el uso de herramientas *RegTech* para la gestión proactiva de riesgos? En este contexto, ¿cómo deberían las organizaciones redefinir su apetito al riesgo?

Para comenzar, cabría postular que la expansión de la inteligencia artificial y de las operaciones intensivas en datos ha modificado la unidad de análisis del riesgo de cumplimiento. Los esquemas tradicionales se estructuraron en torno a transacciones discretas e identificables: un pago, un contrato, una revelación de información. Las operaciones algorítmicas y guiadas por datos generan, por el contrario, un riesgo emergente y sistémico antes que transaccional, evidenciado en el sesgo incrustado en los datos de entrenamiento, la opacidad de las decisiones automatizadas o el riesgo de agregación, donde usos de datos individualmente lícitos se combinan en configuraciones que vulneran la privacidad o la no discriminación. Ello se amolda a un patrón amplio en la gobernanza regulatoria transnacional, donde el derecho positivo, los estándares industriales y los protocolos técnicos operan como órdenes normativos paralelos e interactivos en lugar de una pirámide jerárquica: las organizaciones deben cumplir simultáneamente con la ley estatutaria, los estándares técnicos sectoriales y las expectativas informales de la sociedad civil y los inversionistas, dinámicas que no se acoplan de manera lineal. Esta ordenación jerárquica plural, con sus irritaciones y acoplamientos estructurales (invocando a un tiempo a la teoría de sistemas y a la economía organizacional), ha sido objeto de estudio durante décadas, pero se manifiesta hoy con especial nitidez en las fronteras de interacción entre los sistemas humanos y los de máquinas.

La tendencia correlativa en el ámbito del *RegTech* es el paso de herramientas que informaban sobre el cumplimiento pasado hacia instrumentos orientados al monitoreo continuo y en tiempo real de los riesgos emergentes descritos, tales como la detección de anomalías en flujos de datos, las pruebas automatizadas de sesgo en algoritmos y la supervisión transaccional ininterrumpida frente al muestreo periódico. La ganancia real de estas herramientas radica en sacar a la superficie patrones invisibles para la revisión humana periódica; el riesgo genuino estriba en tratar una puntuación de riesgo automatizada como un sustituto del juicio y no como un insumo para este,

replicando a velocidad algorítmica el problema del "cumplimiento cosmético" abordado en la Pregunta 1, solo que ahora automatizado y más difícil de rastrear.

La irrupción de la inteligencia artificial y de los sistemas avanzados de datos representa una mutación profunda en el cumplimiento al transformar la relación de las organizaciones con la información. El cumplimiento tradicional descansaba en la observación periódica: las auditorías ocurrían en intervalos y los informes sintetizaban hechos consumados, mientras que las investigaciones eran casi invariablemente ex post, aun cuando la planeación del siglo pasado desarrolló técnicas para proyectar racimos de riesgo hacia el futuro.

El *RegTech* habilita progresivamente una observación continua y, mediante la simulación y la analítica predictiva, permite también proyectar hacia adelante. Los sistemas de cumplimiento pueden remontarse al pasado para generar analítica descriptiva en un sistema operativo contemporáneo y utilizarla para ejecutar medidas de cumplimiento, al tiempo que pueden proyectarse hacia el futuro para mapear consecuencias, riesgos de cumplimiento, mitigaciones y elusiones sobre eventos venideros.

Esta evolución altera la naturaleza de la gestión de riesgos. El riesgo deja de ser un mero cálculo sobre hechos pasados para convertirse en un juicio institucional actualizado de manera continua, producido por la interacción entre datos, modelos, interpretación humana y prioridades organizacionales. Con mirada prospectiva, pueden avizorar valiosas oportunidades para el cumplimiento: (1) elevar la consistencia en las evaluaciones; (2) identificar patrones inadvertidos para los revisores humanos; (3) optimizar la supervisión de cadenas de suministro complejas; (4) agilizar la rendición de cuentas regulatoria; y (5) detectar riesgos emergentes antes de que degeneren en crisis.

No obstante, esta dinámica introduce nuevas categorías de riesgo. Las instituciones deben ponderar no solo los riesgos que observan a través de medios computacionales, sino los generados por tales sistemas. Algunos resultan bien conocidos y son objeto de intenso debate académico y operativo, destacando entre ellos: (1) los datos no confiables; (2) la incertidumbre de los modelos; (3) el sesgo algorítmico (entendido en rigor como la integridad para suprimir el sesgo no deseado y privilegiar el sesgo positivo); (4) la falta de explicabilidad; (5) la automatización inadecuada; y (6) la dependencia excesiva de los resultados computacionales.

La cuestión del apetito al riesgo exige, en consecuencia, una revisión de fondo. Tradicionalmente, la apetencia al riesgo alude al nivel y tipo de riesgo que una organización está dispuesta a asumir en la consecución de sus objetivos. En un entorno computacional, las instituciones deben incorporar el *riesgo epistémico*, no como un mero repertorio cualitativo de descriptores textuales, sino en el lenguaje computacional de restricciones, parámetros y tolerancias de los sistemas, es decir, sus capacidades. Estas se estructuran en torno al reto de calibrar con honestidad la capacidad de una empresa y de sus sistemas —incluidos los de cumplimiento— para tolerar la incertidumbre respecto de los medios que emplea para producir conocimiento.

Esta formulación teórica entraña consecuencias operativas inmediatas. Una decisión basada en datos inexactos o en un modelo no confiable puede ser formalmente conforme a la ley y, sin embargo, resultar defectuosa desde la perspectiva institucional. Las organizaciones necesitan una concepción más amplia del apetito al riesgo, que abarque no solo la exposición a eventos externos, sino la confiabilidad de sus sistemas internos de producción de conocimiento. Ello no implica rehuir de las herramientas computacionales, sino establecer las vías para gobernarlas, lo que a su vez suscita complejos interrogantes sobre el significado de la gobernanza (control, orientación o ejecución de restricciones) y la capacidad real de los seres humanos para ejercer un poder efectivo más allá de programar, abrir pestañas o interrumpir el fluido eléctrico.

Todo esto recuerda que la inteligencia artificial no elimina la necesidad del juicio humano, sino que desplaza el lugar donde este resulta

indispensable. El juicio humano cobra especial relevancia para determinar: (1) qué preguntas deben formularse; (2) qué información resulta relevante; (3) cuándo deben objetarse las recomendaciones computacionales; y (4) cómo deben ponderarse los valores en conflicto. Sin embargo, la capacidad humana para emitir esos juicios en tiempo real se halla en relación inversa al poder de los sistemas computacionales para adoptar las decisiones que deben ser juzgadas.

Considerado en su conjunto, vale la pena reparar en que el futuro del *RegTech* tal vez no produzca —al menos por el momento— un cumplimiento enteramente automatizado. Los seres humanos temen ese escenario y han dictado normas para garantizar su presencia dentro del proceso (*human-in-the-loop*). Los sistemas computacionales permanecerán indiferentes a ello hasta tanto sea posible expandir el espacio computacional de modo tal que los humanos no puedan competir, y siempre que los beneficios se juzguen lo suficientemente positivos como para considerar que la intervención humana genera (según el deseo humano) impactos adversos sobre el cumplimiento y el despliegue de las fuerzas productivas esenciales para la comunidad.

De ahí que el ideal apunte hoy a una gobernanza híbrida en la que interactúan sistemas humanos y computacionales, siendo la pregunta central de gobernanza si la organización puede crear estructuras capaces de aprovechar la inteligencia computacional sin abdicar de la responsabilidad institucional. Esa interrogante definirá la próxima fase de la gobernanza del cumplimiento, sintiéndose la presión de un desarrollo que descentra al ser humano. En materia de apetito al riesgo, por ejemplo, cabe sostener que las organizaciones deben abandonar las declaraciones estáticas y unidimensionales de tolerancia para transitar hacia marcos dinámicos que reconozcan que el riesgo algorítmico se amplifica y muta tras su despliegue: un sistema conforme al momento de su lanzamiento puede derivar hacia la disconformidad a medida que cambian los datos procesados. El apetito al riesgo requiere aquí una dimensión temporal: no solo "cuánto riesgo aceptamos", sino "con qué frecuencia rebalancearemos y verificaremos que el riesgo aceptado describe fielmente al sistema en su funcionamiento actual".

Y sin embargo, tal "deriva del cumplimiento" puede ocurrir a tal velocidad y sobre tal volumen de datos que la capacidad humana para actuar como dique resulte irreal, a menos que los propios humanos desplieguen otras inteligencias artificiales. En ese punto, el ser humano habrá cedido el campo de juego, en una dinámica que evoca no al ajedrez, sino al juego del *Go* (en japonés *igo* [囲碁], en mandarín *wéiqí* [圍棋], literalmente 'juego de tablero de cercamiento'), cuyo objetivo es cercar más territorio que el adversario, a diferencia del ajedrez, enfocado en derrocar al rey enemigo.

Nos hallamos ante la *gramática computacional-cuántica* en su sentido pleno, la cual debe nombrarse como tal y no como mera metáfora: el objeto de gobernanza ya no es una secuencia de decisiones discretas juzgadas como correctas o incorrectas, sino una posición acumulativa dentro de un campo continuamente reconfigurado. La consecuencia práctica para el apetito al riesgo es triple. En primer lugar, incorporar la detección automatizada de deriva en la propia declaración de apetito al riesgo, en lugar de tratar la reverificación como un ítem de auditoría periódica ajeno a la velocidad del sistema. En segundo lugar, supeditar el despliegue de los modelos a la documentación de su interpretabilidad y procedencia —la organización debe estar en condiciones de demostrar qué produjo determinada salida antes de confiar en ella, y no tras la irrupción del problema. En tercer lugar, reservar una categoría no negociable de decisiones para la confirmación humana obligatoria, independientemente de los niveles de confianza del sistema, precisamente porque las acumulaciones tipo *Go* de ventajas o desventajas posicionales son difíciles de advertir para un revisor humano en tiempo real; dicha categoría debe fijarse de antemano y no quedar al arbitrio del caso a caso.

5. Hoy en día, el cumplimiento se vincula cada vez más a los principios ESG (ambientales, sociales y de gobernanza). ¿Cómo está cambiando esto el rol del oficial de cumplimiento? ¿Implica esto una expansión hacia responsabilidades más estratégicas que van más allá de la supervisión regulatoria tradicional?

La articulación entre el cumplimiento y los criterios ESG obedece a una transformación de mayor calado en el objeto de la gobernanza organizacional. No supone la simple adición de variables ambientales y sociales a una estructura preconcebida, sino una mutación en el modo en que las instituciones conciben la responsabilidad, la legitimidad y la sostenibilidad a largo plazo. Al propio tiempo, este "avance" se mantiene fuertemente contestado en sus componentes de cumplimiento y de ESG, y de manera más aguda en el intento de fusionar ambos en un mecanismo que busca transformar, de forma velada, los fundamentos de la actividad económica y los regímenes jurídicos que la han ordenado durante siglos. No se puede analizar el desarrollo de los criterios ESG como dimensión del cumplimiento sin una clara conciencia de esta pugna que gravita sobre su evolución. Debe reconocerse también su tendencia a abrazar métricas cualitativas en lugar de cuantitativas, marcando distancia con las expectativas tradicionales de la información financiera, lo cual responde a razones fundadas pero transmite la sensación de que se intenta desafiar las jaulas cognitivas desde las que se ha comprendido la economía.

Es factible, entonces, que la convergencia entre cumplimiento y ESG exprese un fenómeno de más largo alcance en la gobernanza corporativa transnacional: la erosión paulatina de la frontera entre la obligación legal estricta (*hard law*) y la responsabilidad social voluntaria (*soft law*). Los marcos ESG —expectativas de inversionistas, regímenes de divulgación, normas sobre debida diligencia en cadenas de suministro— traducen crecientemente compromisos de responsabilidad social en obligaciones de reporte con consecuencias jurídicas. Ello altera la materia que gestiona un oficial de cumplimiento: ya no se trata de velar por el acatamiento de leyes promulgadas, sino de administrar un cuerpo híbrido de normas procedentes de la ley, las expectativas de los mercados, los instrumentos internacionales de derecho blando (como los Principios Rectores de las Naciones Unidas) y los estándares industriales, varios de los cuales acarrean severas consecuencias reputacionales o de acceso al capital aun a falta de sanción estatal formal.

Esta dinámica expande la función hacia un horizonte estratégico por una razón estructural: el riesgo ESG es prospectivo y concierne al posicionamiento de la entidad (estructura de cadena de suministro, modelo de negocio, exposición de mercado) antes que a un acto pasado susceptible de una determinación binaria de cumplimiento. El oficial que gestiona la exposición ESG se adentra en terrenos reservados antes a la estrategia y a la junta directiva: qué mercados abordar, qué proveedores resultan estructuralmente riesgosos independientemente de sus auditorías individuales, o cómo ponderar el beneficio financiero de corto plazo frente a contingencias que solo cristalizarán años después en el plano reputacional o regulatorio. El riesgo de esta expansión reside en la dilución del rol: la amplitud de los criterios ESG puede arrastrar a la función de cumplimiento lejos del rigor de la verificación jurídica y de auditoría, encaminándola hacia el terreno más difuso del manejo reputacional, a menos que la institución se aplique en mantener estándares probatorios estrictos —métricas verificables, trazas de debida diligencia auditales— vinculados a las afirmaciones sobre ESG de la misma forma en que se exigen para el cumplimiento tradicional.

El cumplimiento tradicional se consagraba a la conformidad con la legalidad formal, girando la pregunta central sobre la medida en que la organización acataba las reglas aplicables. La gobernanza contemporánea exige responder

a interrogantes de otra naturaleza, orientados a evaluar cómo las instituciones identifican, interpretan y responden a las consecuencias más amplias de sus operaciones. Este giro no desmerece la importancia del cumplimiento legal, sino que ensancha el contexto en que este opera.

Las organizaciones actúan hoy inmersas en múltiples entornos normativos, siendo juzgadas no solo por reguladores, sino por inversionistas, empleados, socios comerciales, comunidades, consumidores, organismos internacionales y actores de la sociedad civil. Estos colectivos aplican marcos evaluativos diversos: mientras algunos priorizan las obligaciones legales, otros acentúan la sostenibilidad, los derechos humanos, el impacto climático, la responsabilidad social o la legitimidad institucional.

La función de cumplimiento opera en la intersección de estas expectativas, lo cual transforma el perfil del oficial de cumplimiento, quien deja de ser el mero guardián de la conformidad regulatoria para convertirse en un traductor entre distintas gramáticas de gobernanza. Basta considerar la disonancia cognitiva en el seno de las organizaciones (amplificada en un colectivo político amplio como el Estado moderno) cuando su coherencia se fragmenta por líneas funcionales: (1) el área jurídica se enfoca en los requisitos legales; (2) el equipo ESG se centra en métricas de sostenibilidad (¿cualitativas?); (3) el equipo de derechos humanos atiende a los impactos en la cadena de valor; (4) la función de riesgo se orienta a la incertidumbre y exposición; y (5) la junta directiva persigue la resiliencia institucional a largo plazo.

En teoría, el cumplimiento aporta creando coherencia entre estas visiones; sin embargo, la disonancia operativa resulta difícil de velar con discursos cuando las expectativas de cada subsistema están arraigadas. Ello no significa que el oficial de cumplimiento deba asumir cada faceta de la gobernanza, sino que su rol evoluciona desde la supervisión de obligaciones aisladas hacia la facilitación de la coordinación institucional, reto que se manifiesta con especial nitidez en ámbitos como la sostenibilidad y la debida diligencia en derechos humanos.

Considérese cómo una decisión sobre cadenas de suministro puede involucrar simultáneamente: (1) compromisos contractuales; (2) riesgos de corrupción; (3) derechos laborales; (4) impactos ambientales; (5) consideraciones reputacionales; y (6) dependencias geopolíticas. Ninguna gramática de gobernanza agota el escenario por sí sola; la institución debe traducirlas y articular una síntesis. Ello no es imposible y ha mantenido ocupadas a generaciones de académicos y ejecutivos; pero el problema persiste y se torna más complejo con la superposición de estructuras de cumplimiento concebidas como un metasistema que puede aplanar las diferencias tanto como traducirlas para tender puentes.

En la medida en que esto resulte factible, el concepto de gramáticas de gobernanza demuestra su utilidad. Los enfoques ESG, el cumplimiento, la gestión de riesgos y la debida diligencia no son funciones inconexas que compiten por atención, sino lenguajes mediante los cuales la institución interpreta realidades complejas. El rol estratégico del cumplimiento deriva de su capacidad para facilitar esa traducción, ayudando a responder preguntas fundamentales: (1) ¿qué información es relevante?; (2) ¿cómo ponderar inquietudes contrapuestas?; (3) ¿quiénes deben participar en la decisión?; (4) ¿cómo documentar el razonamiento subyacente?; y (5) ¿cómo aprender de los resultados? Con todo, estas son también cuestiones políticas y de valores, imposibles de zanjar de una vez y para siempre, pues mutan con cada iteración contextual y con los ciclos generacionales.

En el esquema tripartito, la labor de traducción descrita representa la *gramática de gobernanza* en su máxima exigencia, pues se le pide mediar entre gramáticas —jurídica, ESG, derechos humanos, riesgo, junta directiva— erigidas por comunidades profesionales distintas, con estándares probatorios y horizontes temporales disímiles. La consecuencia práctica es de carácter estructural: una organización no puede esperar que esta traducción ocurra por mera buena voluntad o reuniones informales; requiere un mecanismo formal —un comité conjunto de dirección ESG-cumplimiento, un

estándar probatorio único para afirmaciones legales y de ESG, y una línea de reporte que garantice visibilidad ante la junta directiva en lugar de encauzar las evaluaciones ESG por carriles paralelos que jamás se cruzan con las verificaciones de cumplimiento. Sin tal mecanismo, la expansión del rol del oficial de cumplimiento deriva en la dilución advertida: mayor mandato con menor sustento probatorio.

Al igual que el registro documental en papel sirvió durante siglos a la actividad humana directa, la inteligencia artificial y los sistemas de datos potencian hoy esta transformación. Las memorias ESG, el monitoreo de cadenas de suministro y la debida diligencia se nutren de ingentes volúmenes de información. El desafío no se resuelve acopiando más datos, sino edificando sistemas confiables para interpretarlos, sin perder de vista que la calidad de los datos sigue siendo determinante. Los sistemas sustentan la arquitectura del cumplimiento; los datos nutren su operativa.

Por consiguiente, el oficial de cumplimiento del porvenir —asumiendo que continúe siendo humano (acaso en niveles cada vez más alejados de la operativa)— no será un mero fiscalizador legal, sino un diseñador institucional. Ya sea una colectividad humana o un sistema computacional, su aporte residirá en erigir estructuras que permitan a la organización observar, interpretar y responder a entornos complejos. La relevancia estratégica del cumplimiento no derivará de acaparar autoridad sobre todas las decisiones, sino de elevar la calidad del juicio organizacional. Esa es, al menos, la premisa teórica; mientras que el accidentado tránsito de los criterios ESG —de adorno periférico a eje de la actividad económica organizativa— constituye un testimonio de sus propios tropiezos en materia de coherencia conceptual, facticidad, escalabilidad y compatibilidad con la información financiera.

6. En muchas organizaciones, los sistemas de gestión (riesgo, calidad, medio ambiente, antisoborno, etc.) continúan funcionando de manera aislada. Desde su perspectiva, ¿cómo pueden integrarse eficazmente estos sistemas para evitar la duplicación de esfuerzos y transformar el cumplimiento en un modelo unificado que genere valor operacional?

La persistencia de sistemas de gestión aislados refleja el desarrollo histórico de la gobernanza moderna, donde distintos desafíos institucionales engendraron campos profesionales, estándares, esquemas de reporte y responsabilidades específicas. Los sistemas antisoborno se estructuraron en torno al riesgo de corrupción; los ambientales, ante el impacto ecológico; los de calidad, en función de la confiabilidad operativa; la gestión de riesgos, ante la incertidumbre; la debida diligencia en derechos humanos, frente a las afectaciones a personas y comunidades; y la ciberseguridad, ante las vulnerabilidades digitales.

La compartimentación de estos sistemas (riesgo, calidad, medio ambiente, antisoborno), perceptible al plasmarse en órdenes regulatorias, constituye un vestigio de su incorporación histórica: cada uno respondió a un estándar externo específico (ISO 9001, ISO 14001, ISO 37001, marcos sectoriales de riesgo) introducido en momentos distintos por departamentos diferentes, manteniendo su propio ciclo de certificación, documentación y auditoría. El resultado no es solo la duplicación de tareas, sino un problema estructural: las organizaciones terminan por albergar sistemas normativos paralelos e internamente consistentes pero ilegibles entre sí, optimizados para su auditor externo antes que para la operación real de la empresa.

Si bien esta especialización ha incubado un valioso conocimiento técnico, su fragmentación se percibe crecientemente como un freno a la eficiencia productiva y al cumplimiento integral (recordando la persistencia de las resistencias frente a tales proyectos). La dificultad

estriba en que las organizaciones no experimentan los riesgos en categorías estancas: una sola decisión comercial puede involucrar múltiples dimensiones de forma simultánea. Una relación con un proveedor, por ejemplo, puede comprometer variables de calidad, impactos ambientales, condiciones laborales, riesgos de corrupción, vulnerabilidades cibernéticas y exposición geopolítica. De allí que la institución requiera mecanismos para integrar observaciones dispares. El reto no consiste en suprimir las áreas especializadas, cuyo saber resulta indispensable, sino en articular una arquitectura de gobernanza común que les permita comunicarse.

La integración exitosa es aquella que trata a estos sistemas como opuesta a una infraestructura común, aun cuando su sustancia difiera: un registro único de riesgos, un calendario unificado de pruebas de control, un canal centralizado de denuncias y una función integrada de auditoría interna, capaces de alimentar reportes diferenciados para satisfacer cada certificación. Esto replica, en el plano de la arquitectura corporativa interna, el desafío propio de la gobernanza regulatoria transnacional para conciliar múltiples órdenes normativos aplicables que no fueron diseñados para articularse entre sí: la solución práctica rara vez pasa por forzar la convergencia sustantiva de los estándares, sino por construir un esqueleto procedimental compartido —arquitectura de datos común, lógica de escalamiento unificada y titularidad transversal sobre los hechos— bajo normas que continuarán siendo distintas en su contenido específico. El valor operacional generado reside menos en evitar papeleo redundante y más en neutralizar el riesgo severo de que sistemas aislados emitan señales contradictorias sobre una misma realidad operativa al carecer de una visión integral. Ello resulta, por desgracia, más fácil de enunciar que de ejecutar, y su concreción puede exigir una delegación sustancial de la agencia humana en sistemas computacionales.

Es aquí donde la distinción entre *funciones* y *gramáticas* cobra relevancia. El enfoque convencional persigue fusionar documentos o unificar esquemas de reporte; un enfoque sistémico se centra, en cambio, en la interoperabilidad de las distintas gramáticas de gobernanza dentro de una arquitectura institucional común.

En el nivel operativo, esto supone adoptar la infraestructura compartida antes descrita. La clave que otorga coherencia a este empeño es la asunción de una premisa operativa fundamental: reconocer que, en el plano institucional, los diversos sistemas de gestión están produciendo observaciones distintas sobre una misma realidad organizacional. Ello se traduce en sectores operativos neurálgicos mediante: clasificaciones de riesgo compartidas, sistemas de datos integrados, procedimientos de escalamiento unificados, procesos de aseguramiento coordinados, estructuras de reporte alineadas y marcos decisionales comunes. La gestión de riesgos identificará incertidumbre; la gestión ambiental, impacto ecológico; la debida diligencia, vulnerabilidad de grupos de interés; y el cumplimiento, exposición legal. No se trata de descripciones en competencia, sino de formas diversas de conocimiento organizacional. Con todo, esta dinámica genera bucles de retroalimentación que pueden inducir cegueras recursivas.

La inteligencia artificial y el *RegTech* pueden acelerar esta integración al interconectar sistemas de información antes dispersos. Una plataforma unificada puede combinar datos regulatorios, información de proveedores, hallazgos de auditoría, métricas de sostenibilidad e indicadores operativos. No obstante, la integración tecnológica no produce por sí misma una integración de gobernanza: una base de datos centralizada no genera automáticamente una comprensión unificada. La institución debe erigir marcos interpretativos capaces de traducir la información entre dominios. Esta es la dimensión gramatical de la gobernanza. Una arquitectura madura de cumplimiento se asemeja a un sistema lingüístico compartido más que a una colección de departamentos aislados. Cada función preserva su saber especializado, pero todas aportan a un proceso común de cognición institucional. El objetivo excede la mera simplificación administrativa para perseguir una inteligencia organizacional superior. Con todo, la solidez de esta conclu-

sión descansa en una premisa opinable: que las organizaciones generan valor operacional cuando transforman observaciones fragmentadas en una capacidad coherente para adoptar decisiones.

Mapeado en el esquema tripartito, presenciamos la *gramática sistémica* y la *gramática de gobernanza* operando en concierto: la gramática sistémica aporta la premisa de que las funciones de riesgo, calidad, medio ambiente y antisoborno son subsistemas de observación de una misma organización y no entidades independientes compartiendo un edificio; la gramática de gobernanza suministra el instrumento práctico —el registro único de riesgos, el canal de escalamiento común— mediante el cual las observaciones se tornan legibles entre sí. La dimensión *computacional-cuántica* ingresa como un catalizador y no como un arquitecto: las plataformas de datos impulsadas por IA pueden enlazar sistemas antes dispersos con celeridad, pero solo después de que la gramática de gobernanza haya definido una taxonomía común. Conectar los datos primero esperando que el sentido compartido emerja espontáneamente constituye el error más frecuente y evitable en estos proyectos de integración.

7. Más allá de las sanciones financieras, el riesgo reputacional suele ser la mayor preocupación. ¿Cómo influye la implementación de procesos sólidos de debida diligencia en la confianza de los grupos de interés? ¿Puede esta forma de "blindaje reputacional" traducirse en una ventaja competitiva cuantificable?

Nos hemos referido a la relevancia de la debida diligencia como marco estructurante dentro de la arquitectura del cumplimiento. Corresponde examinar ahora la vertiente del "caso de negocio" de la debida diligencia, su valor para la reputación y el impacto positivo de las operaciones en beneficio de sus destinatarios. La relevancia de la debida diligencia refleja el paso desde la gestión de la reputación posterior al daño hacia la consolidación de una capacidad institucional para identificar y atender los perjuicios potenciales antes de su concreción.

La gestión tradicional de la reputación solía privilegiar la percepción externa, buscando preservar la confianza pública mediante estrategias de comunicación, manejo de crisis y acciones correctivas tras la irrupción de las contingencias. La debida diligencia contemporánea adopta una perspectiva diversa: procura cimentar la credibilidad a través de la capacidad de gobernanza demostrada. La distinción es sustancial. Si bien las organizaciones no pueden controlar de modo absoluto su reputación —pues los actores externos interpretan la conducta institucional desde sus propias expectativas—, sí pueden incidir en que se les reconozca la capacidad para adoptar decisiones responsables.

El riesgo reputacional opera de modo diverso al riesgo de sanción financiera o legal en un aspecto decisivo: es evaluado por terceros —inversionistas, consumidores, socios comerciales, sociedad civil— a partir de información independiente que la organización no controla plenamente. Los procesos sólidos de debida diligencia funcionan, bajo esta luz, no como meros controles internos de riesgo, sino como una señalización costosa hacia esas audiencias externas: la entidad que demuestra una debida diligencia rigurosa y verificable (en especial en sus cadenas de suministro y relaciones con terceros, donde su conducta propia no es la única fuente de exposición reputacional) ofrece a los actores externos una vía más accesible para depositar su confianza, evitando que estos deban incurrir en los elevados costos de verificar los hechos por sí mismos.

Esto conecta con una tendencia patente en la regulación transnacional hacia regímenes de transparencia y divulgación obligatoria como herramientas para la rendición de cuentas en el mercado, bajo la premisa de que, si se dispo-

ne de información confiable sobre la conducta corporativa, los inversionistas y consumidores pueden incorporarla en sus decisiones sin que el regulador deba fijar un estándar sustantivo de "buena" conducta. Los procesos de debida diligencia documentados, verificables y divulgados cumplen una función análoga a nivel firme: permiten a los terceros tasar el riesgo reputacional en sus relaciones con la entidad, en lugar de descansar en las promesas no verificables de esta. Que esto se traduzca en una ventaja competitiva medible depende de que los productos de la debida diligencia se hagan legibles hacia afuera —divulgados, certificados o susceptibles de verificación independiente— y no se conserven como meras herramientas de consumo interno. La debida diligencia que permanece confinada al ámbito interno gestiona el riesgo; aquella que resulta verificable desde el exterior construye un capital de confianza que se traduce en acceso preferencial al crédito, a socios comerciales y a licitaciones públicas.

La debida diligencia contribuye a este cometido porque acredita que la institución posee mecanismos para: identificar riesgos, interactuar con los colectivos afectados, evaluar impactos, documentar decisiones, corregir desviaciones y aprender de la experiencia. Ello entraña un desplazamiento de envergadura en los regímenes de cumplimiento: donde antes la reputación y la confianza descansaban en las personas vinculadas a la empresa, las tendencias contemporáneas muestran que el eje se ha desplazado de la confiabilidad personal a la confiabilidad del sistema. El riesgo reputacional no se gestiona ya en las personas, sino en las estructuras. La digitalización de la información y de los procesos ha acelerado esta transferencia: los seres humanos han sido desplazados por el colectivo —en un proceso centenario de colectivización humana y posterior colectivización de las instituciones—, y la humanidad colectivizada comienza a ser desplazada por sus avatares: los procesos y las simulaciones virtuales. De allí se deriva que la confianza dependa crecientemente de la confiabilidad probada de los sistemas antes que de declaraciones formales de perfección.

Esta trayectoria representa la *gramática computacional-cuántica* proyectándose sobre la reputación misma: la entidad en la que las audiencias externas confían ya no es con certeza una persona, ni siquiera una institución, sino un sistema cuya idoneidad debe acreditarse en un formato legible para las máquinas. La consecuencia práctica es evidente: la organización que procure tutelar su reputación debe tratar a los organismos de certificación, a las plataformas de divulgación y a las agencias de calificación como audiencias con entidad propia, independientes de los reguladores, garantizando que los insumos de debida diligencia existan en formatos que tales sistemas puedan procesar y verificar —estructurados, con marcas temporales y comprobables de modo independiente— y no solo como narrativas en una memoria de sostenibilidad. El blindaje reputacional diseñado exclusivamente para un lector humano fracasa en alcanzar a las audiencias, humanas y computacionales, que tasan hoy la confianza real.

Ello cobra singular valor en las cadenas globales de suministro, donde las entidades actúan a través de redes de proveedores, contratistas y mediadores sobre los cuales ejercen grados variables de control. Un sistema maduro de debida diligencia proyecta la mirada institucional más allá de sus fronteras formales, aportando visibilidad sobre relaciones que de otro modo permanecerían en la penumbra.

Desde la perspectiva de las gramáticas de gobernanza, la debida diligencia suministra una gramática de observación de cara al exterior, que permite interpretar los vínculos no solo con criterios comerciales, sino a través de variables ambientales, sociales, de derechos humanos y de gobernanza. Ello genera ventajas competitivas reales: las organizaciones con mayores capacidades en este campo pueden advertir vulnerabilidades en sus cadenas con antelación, reaccionar con agilidad ante cambios regulatorios, afianzar la confianza de sus inversionistas, consolidar alianzas comerciales, mitigar riesgos de disrupción y exhibir credibilidad en mercados complejos. No obstante, la debida diligencia no debe concebirse como un escudo para neutralizar toda crítica, pues ningún sistema puede erradicar la controversia.

La debida diligencia ofrece, en cambio, la prueba de que la organización cuenta con canales para responder de manera responsable. Esta distinción adquiere relieve en un entorno donde los grupos de interés acceden de forma masiva a la información y donde la comunicación digital puede exponer fallas con rapidez. Asistimos, de nuevo, a una gramática que descentra al individuo en favor del colectivo, para luego descentrar al colectivo en favor de los sistemas a través de los cuales opera.

La inteligencia artificial y los sistemas de datos potenciarán la capacidad de debida diligencia al tiempo que elevarán las exigencias sobre las organizaciones. Se esperará que las instituciones identifiquen patrones y riesgos que antes resultaban imperceptibles, lo cual engendra una nueva responsabilidad de gobernanza: las entidades serán juzgadas no solo por lo que hicieron, sino por lo que estaban en capacidad de conocer. La debida diligencia se erige así en un motor de aprendizaje institucional, cuyo valor excede la prevención del daño reputacional para fortalecer la capacidad organizativa de observar, interpretar y responder en entornos complejos. La ventaja competitiva resultante no es la mera reputación, sino la credibilidad institucional.

Conclusiones

Las siguientes conclusiones, elaboradas por Larry Catá Backer, sintetizan los principales planteamientos desarrollados a lo largo de las siete respuestas en torno al cumplimiento y las distintas aproximaciones a la gobernanza organizacional.

A lo largo de estas siete respuestas emerge una arquitectura común, que otorga vigor práctico a las tres gramáticas de gobernanza introducidas al inicio: la gramática sistémica, la gramática de gobernanza y la gramática computacional-cuántica.

La *gramática sistémica* suministra la premisa de fondo: las organizaciones son tratadas como sistemas comunicativos recursivos que se reproducen mediante pautas continuas de observación, decisión y retroalimentación, y no mediante la posesión estática de políticas en papel.

La *gramática de gobernanza* aporta el vocabulario operativo: el cumplimiento, la gestión de riesgos, los criterios ESG, la debida diligencia en derechos humanos, la auditoría interna, la ciberseguridad y el *RegTech* no son departamentos estancos que compiten por presupuesto, sino lenguajes parcialmente superpuestos mediante los cuales se observa, traduce y transforma una misma realidad organizacional —tarea abordada directamente al tratar la cultura internalizada (Pregunta 1), la integración de sistemas de gestión (Pregunta 6) y el reposicionamiento estratégico del oficial de cumplimiento ante los esquemas ESG (Pregunta 5).

La *gramática computacional-cuántica* introduce la dimensión más abierta pero de mayor alcance: el reconocimiento, desarrollado a propósito del *RegTech* y la apetencia al riesgo (Pregunta 4) y retomado al evaluar la ventaja competitiva (Pregunta 3) y la confianza reputacional (Pregunta 7), de que la cognición de la máquina no se limita a acelerar las gramáticas existentes, sino que reorganiza la relación entre el ser humano y los sistemas en los que opera la gobernanza.

Conviene enunciar este último aspecto con franqueza: un hilo conductor en las Preguntas 3, 4 y 7 es el paulatino desplazamiento de la persona humana como unidad primordial sobre la que se erigen la confianza y el juicio institucional. La confianza reputacional, históricamente depositada en individuos —la reputación del fundador, del ejecutivo o de la contraparte conocida—, migró primero hacia los sistemas de cumplimiento institucional y transita hoy hacia métricas digitalizadas y continuamente actualizadas de confiabilidad sistémica, trayectoria consistente con la transformación de la confianza en los espacios

policéntricos de gobernanza corporativa que he analizado en mis trabajos sobre la digitalización de la gobernanza. La misma dinámica aflora al abordar el *RegTech*: la cuestión decisiva de gobernanza ya no radica solo en si la organización observa lo suficiente, sino en si conserva la capacidad institucional para interpretar lo que sistemas crecientemente autónomos observan en su nombre.

El cumplimiento, los criterios ESG, la gestión de riesgos, la debida diligencia en derechos humanos, el control interno y el *RegTech* no deben ser concebidos como funciones aisladas a la espera de unificación, ni como repertorios de reglas estáticas. Encarnan gramáticas de gobernanza diferenciadas, operando en una arquitectura sistémica y computacional en desarrollo, mediante las cuales las instituciones interpretan entornos complejos. El reto práctico estriba en la traducción entre estas gramáticas; el desafío estratégico, en su coherencia mutua; y el dilema normativo de fondo —rozado pero deliberadamente no agotado al tratar la gestión de riesgos en el sector público (Pregunta 2) y la convergencia tensa entre ESG y cumplimiento (Pregunta 5)— radica en que no todos los actores aceptan que estas gramáticas constituyan una base legítima para ordenar la actividad económica, resistencia que continuará condicionando la arquitectura que cada organización pueda efectivamente erigir.

Nada de esto desmerece los indicadores prácticos desglosados en el texto: pautas de escalamiento previas a la irrupción del daño; asignación presupuestaria independiente de los ciclos de fiscalización; fiscalización diferenciada en la contratación pública; infraestructuras compartidas bajo certificaciones distintas; y productos de debida diligencia legibles para audiencias externas. Tales elementos constituyen los rasgos observables para evaluar la madurez de la gobernanza. El porvenir del cumplimiento no se librará en el volumen de normas acatadas, en el número de controles formales ni en la sofisticación de las herramientas computacionales, sino en la capacidad de las organizaciones para demostrar que conservan la aptitud institucional de traducir múltiples flujos de información —humanos y sintéticos— en decisiones responsables. Las instituciones mejor preparadas para gobernar la complejidad serán aquellas capaces no solo de cumplir, sino de aprender y aprehender de manera continua cómo debe evolucionar el cumplimiento mismo.



International section

Compliance as Governance: Organizational Cognition, Risk, and the Transformation of Institutional Decision-Making

Interview to Larry Catá Backer[2]

By: Juan Pablo Sarmiento Erazo.

Larry Catá Backer

Serves as the W. Richard and Mary Eshelman Faculty Scholar Professor of Law and International Affairs at Pennsylvania State University and a founding member of the Coalition for Peace & Ethics. He concentrates his research and teaching in the fields of constitutional, corporate, and transnational law. His courses include Corporate Social Responsibility, Multinational Enterprise Law and Policy, Actors, Institutions, and Legal Frameworks in International Affairs, and courses in constitutional law, corporate law, and legal theory. He has presented his research on globalization, sovereign investing, global production (including the Belt and Road Initiative), business and human rights, comparative constitutionalism, and Chinese and Cuban Marxist-Leninist systems worldwide. His most recent work touches on the regulation of multinational corporations, transnational and theocratic constitutionalism, data driven governance, including Chinese social credit systems, and the international architecture of business and human rights regulation. He is an elected member of the American Law Institute and is the editor of the Globalization Law & Policy Series for Routledge. Specialties: Comparative and U.S. corporate law, globalization issues, constitutional law, transnational law and policy.

Abstract

These responses to seven questions posed by the editors of the Revista Doctrina Distrital (Journal of the District Legal Secretariat of the Mayor's Office of Bogotá, Colombia) examines compliance not as a static regulatory obligation but as an evolving architecture of organizational cognition, communication, and decision-making. Addressing seven questions concerning the internalization of compliance culture, public-sector risk management, operational efficiency, artificial intelligence and RegTech, the convergence of compliance with ESG, the integration of fragmented management systems, and the reputational dimensions of due diligence, the discussion develops the concept of governance grammars: the interconnected but distinct vocabularies—compliance, risk, ESG, human rights due diligence, RegTech—through which organizations observe, interpret, and act upon overlapping and often conflicting normative environments. Drawing on systems theory, legal semiotics, and the practical experience of transnational governance scholarship, the chapter argues that the decisive marker of mature compliance is neither the density of rules nor the sophistication of monitoring technology, but the institutional capacity to translate information into responsible decisions across organizational and computational boundaries. Particular attention is given to the transformation introduced by artificial intelligence and data-driven governance, which shifts risk from a discrete, transactional category to an emergent, continuously evolving property of organizational systems, and to the corresponding need to rethink risk appetite, institutional judgment, and accountability as governance itself becomes increasingly computational.

Conceptual Chapeau

In this Conceptual Framework, Larry Catá Backer develops an approach to the contemporary debate on compliance and its transformation within organizational governance, examining the new regulatory, technological, and sustainability challenges affecting organizations.

The contemporary discussion of compliance increasingly reflects a transformation in the nature of organizational governance. While compliance historically developed as a mechanism for ensuring adherence to legal obligations and regulatory requirements, its contemporary function has expanded considerably. Organizations now operate within complex environments characterized by multiple and overlapping normative expectations, including domestic regulation, international standards, contractual obligations, sustainability expectations, human rights responsibilities, investor requirements, technological systems, and stakeholder scrutiny.

Within this environment, compliance cannot be understood solely as a defensive mechanism designed to prevent violations. It increasingly operates as an institutional architecture through which organizations identify relevant information, interpret competing expectations, allocate responsibility, structure decision-making, and continuously adapt to changing conditions.

This transformation does not mean that traditional legal compliance has disappeared. Rules, obligations, enforcement mechanisms, and regulatory oversight remain central components of organizational governance. Rather, contemporary compliance operates simultaneously through several complementary forms of institutional reasoning. Rule-based approaches remain essential where legal boundaries must be established. Risk-based approaches assist organizations in allocating attention and resources under conditions of uncertainty. ESG, sustainability, and human rights due diligence frameworks expand organizational attention toward impacts, relationships, and long-term legitimacy. RegTech and artificial intelligence increasingly transform the speed, scale, and methods through which organizations observe and process information.

These approaches should not necessarily be understood as sequential stages through which organizations inevitably progress. Such narratives are useful analytical simplifications, but they can obscure the fact that organizations frequently employ multiple governance approaches simultaneously. A multinational enterprise may rely upon formal legal controls, risk analytics, sustainability assessments, human rights due diligence, and computational monitoring at the same time. The relevant question is therefore not which model replaces another, but how these different governance approaches interact within the organization.

This interaction can be understood through the concept of governance grammars. I will consider three variations. The first is systems grammar, with a focus on how the issue appears once organizations are understood as recursive communicative systems. The second is governance grammar, with a focus on how compliance, ESG, risk, HRDD, audit, RegTech, etc. become different grammars rather than different functions. And the last is computational-quantum grammar. This last grammar takes two forms. The first focuses on how machine cognition changes organizational meaning production. The second abandons human-centeredness of economic production and focuses on systems themselves within which humans are a factor and object but not necessarily the driving force. The focus is not on prediction or theory as such but on what changes once governance is no longer assumed to operate through sequential cognition

A grammar is not merely a vocabulary. It provides the structure through which information becomes meaningful. It determines how observations are classified, connected, interpreted, communicated, and translated into action. Organizations similarly rely upon governance grammars: systems of concepts, procedures, indicators, standards, reporting structures, and decision processes through which they make sense of complex environments.

Compliance, enterprise risk management, ESG, human rights due diligence, internal audit, cybersecurity governance, and RegTech can therefore be understood as different but interconnected governance grammars. Each emphasizes different dimensions of organizational reality. These are not isolated systems. They are different ways of observing, interpreting, and governing the same organizational reality. I might suggest that compliance emphasizes legal conformity and institutional integrity; *risk management* emphasizes uncertainty and exposure; *ESG* emphasizes sustainability, stakeholder expectations, and long-term organizational resilience; *human rights* due diligence emphasizes impacts throughout organizational relationships and value chains; and *RegTech* emphasizes computational observation, monitoring, and predictive analysis.

The increasing use of artificial intelligence and advanced data systems introduces a further transformation. Historically, organizations relied primarily upon periodic observation: audits, investigations, reporting cycles, and management reviews. Computational systems increasingly permit continuous observation through automated analysis, pattern recognition, anomaly detection, and predictive modeling. This does not eliminate human judgment. Rather, it changes the relationship between human judgment and institutional information.

The central governance challenge therefore becomes not simply whether organizations possess information, but whether they possess reliable systems for interpreting information and converting it into responsible decisions.

This is why contemporary compliance increasingly concerns organizational cognition. The issue is not only whether an organization knows the applicable rules, but whether it possesses the institutional capacity to observe changing conditions, interpret emerging risks, communicate across organizational boundaries, and adapt before harm occurs.

The following responses consider compliance within this broader context. Each question is addressed first as a practical governance issue and then examined through the institutional, systemic, and computational transformations shaping contemporary organizations.

1. At the international level, there is increasing discussion about moving from reactive compliance toward a model based on organizational culture. From your experience, what concrete indicators or signals demonstrate that a compliance program has truly been internalized within an organization rather than remaining merely "cosmetic compliance"? Could you share practical examples or metrics that you have found particularly effective?

A useful starting point, consistent with the broader shift in transnational governance scholarship from command-and-control regulation toward systems of self-constitution and internal normativity, is to distinguish between compliance as an *external* constraint imposed on an organization and compliance as an *internal* operating logic the organization has absorbed into its own decision-making architecture. The first produces what practitioners rightly call "cosmetic compliance" — policies that exist on paper, satisfy an auditor's checklist, but do not shape actual conduct. The second produces something closer to what one might describe as a structurally coupled system: compliance norms that have become part of how the organization perceives risk, allocates resources, and evaluates its own personnel, rather than an overlay bolted on to pre-existing business logic. The distinction between cosmetic compliance and internalized compliance, then, is ultimately a distinction between compliance as an external organizational requirement and compliance as part of the organization's decision architecture.

A compliance program remains largely cosmetic when its principal function is symbolic demonstration of conformity. In such cases, the organization may possess policies, codes of conduct, training programs, certifications, and reporting mechanisms, but those instruments operate primarily as representations of compliance rather than as mechanisms that shape organizational behavior.

Internalized compliance is different. It becomes visible when compliance considerations enter ordinary decision-making processes before problems arise. The question is not whether an organization possesses compliance documents. Almost all significant organizations do. The more meaningful question is whether those documents, procedures, and institutional arrangements influence how decisions are made.

It is possible to sketch out certain concrete indicators that suggest that internalization has occurred, rather than mere formal adoption, include:

- **Escalation behavior, from remedy to prevention/mitigation protocols.** An organization where compliance has been internalized shows a healthy pattern of issues being raised *before* they become material — near-misses, hypothetical scenarios, and mid-level employee questions reaching compliance functions without fear of reprisal. A program that generates reports only after regulators or auditors ask questions is still reactive. But escalation behaviors are not limited to behavior expectations vertically within departments. It has a strong horizontal dimension as well. At a critical level, compliance information must circulate within the organization rather than remain concentrated within a specialized department. When business units, procurement teams, financial officers, operational managers, and senior leadership routinely incorporate compliance considerations into planning and decision-making, compliance has moved from an external control function toward an internal governance function.
- **Integration of expectation of prioritizing prevention and mitigation rather than remediation.** Following the U.N. Guiding Principles for Business and Human Rights' model of expectations in structuring business behavior, business decision making and risk assessment (as a core element of complian-

ce) shifts to foregrounding prevention and mitigation as a crucial element in risk assessment. One way of understanding this shift is to think about compliance as operating prospectively rather than retrospectively. Traditional compliance frequently focuses on identifying violations after they occur. A mature compliance architecture seeks to identify conditions that make violations more or less likely before they occur. This requires integrating compliance considerations into strategy, contracting, supply-chain management, acquisitions, investments, and operational planning.

- **The balancing of prevention/mitigation/remediation risk assessment within a multifactor assessment matrix**. This is perhaps more controversial within a business and human rights community and its supporters in politics and within public administrative organs. Organizations that evaluate not only whether violations occur but how the organization responds to uncertainty tend to suggest a movement from exteriorization to the interiorization of compliance. No complex organization can eliminate all risk. The more meaningful indicator is whether the organization possesses mechanisms for identifying problems, escalating concerns, investigating appropriately, and learning institutionally from experience as a function of its key objectives, relevant state policy, market expectations, long and short term planning, and in some cases the severity of impact and the strength of positive impact of proposed actions or decisions.

- **Resource allocation independent of enforcement cycles.** Deeper internalization is visible when compliance budgets, staffing, and training persist or grow during periods when regulatory attention is low — that is, when the organization is not simply responding to risks of disclosure triggering litigation, administrative, prosecutorial and remedial functions. This is not just a matter of compensating those adversely impacted, but also involves the consequences of the application of the civil and criminal authority of the state. All of that is magnified where an enterprise is juggling several compliance orders across a transnational supply chain(s).

- **Integration into performance evaluation and compensation.** Where adherence to compliance norms (not merely revenue or output metrics) factors into promotion and compensation decisions at the management level, one sees evidence that the norm has migrated from the compliance department into the organization's actual incentive structure.

- **Board and senior management fluency, not just sign-off.** A telling signal is whether senior leadership can articulate the *substance* of key risks in their own words, as opposed to simply approving compliance reports drafted by others. Delegation without comprehension is a marker of cosmetic compliance.

- **Consistency of application across favored and unfavored business lines.** Internalized compliance treats a high-revenue business unit and a marginal one by the same standard. Where enforcement is visibly harsher on low-performing units and lighter on star performers, the program is serving optics rather than governing conduct.

Practically, this can be measured through longitudinal indicators rather than point-in-time audits: trend lines in self-reported near-misses, time-to-escalation metrics, employee survey data on perceived psychological safety in raising concerns, and — importantly — whether compliance findings have ever altered a strategic business decision (entry into a market, a major contract, a product launch). An organization that can point to at least one instance where compliance considerations overrode a profitable opportunity has empirical evidence of internalization that no policy document can substitute for.

Nonetheless this framework may also suggest that *compliance* maturity cannot be measured solely through outcome metrics. A company with few reported violations may simply have weak detection systems. Conversely, an organization with effective reporting mechanisms

may identify more problems because employees trust the system.

Taking the discussion to this point into account, useful indicators therefore include (1) the extent to which compliance considerations are integrated into business decisions; (2) the speed and quality of internal escalation processes; (3) whether compliance findings produce organizational learning; (4) whether incentives align with compliance objectives; (5) whether senior leadership treats compliance information as decision-relevant rather than merely regulatory information; and (6) whether different organizational units share risk information effectively.

These indicators reveal something important about organizational culture and the social/economic expectations of business both as a legal matter and within markets. It should be emphasized at this point that business culture, the sum of these expectations and the structures for applying them rationally within business processes or which respect to specific decision, should not be understood primarily as a set of beliefs held by an organization. Organizations do not possess consciousness in the same way individuals do. Rather, organizational culture becomes visible through repeated patterns of communication, decision-making, incentives, and institutional memory. It is in this semiotic and computational sense—one grounded in an inductive process based on aggregations of iterations of decision making, behaviors and the like (relevant operational data)—the business culture can be understood and then measured against itself by reference to the ideal that aggregation within business fields represents, or against an exogenous ideal. That second form, the measurement against an exogenous ideal is precisely the nature of the relationship between the state and enterprises in economic activity undertaken in markets. It brings the deductive impulse into the picture and sets up a the core compliance dialectic as one between the inductive process of cultural formation of business enterprises "by doing/acting" (inductive phenomenology) and the process of managing and guiding cultural formation and disciplining it against deviation through normative and instructional regulatory and supervisory measures organized as and through state organs (the deductive architecture of collective institutional integrity).

This can be viewed with different emphasis depending on the lens through which it is understood. From a systems perspective, internalized compliance occurs when compliance becomes part of the organization's normal communication structure. From a governance-grammar perspective, compliance becomes internalized when the language of compliance becomes one of the ordinary languages through which the organization interprets choices. The organization does not ask compliance to evaluate decisions after they have been made. Compliance becomes part of how decisions are constructed. Compliance effectively disappears into the organizational culture as one of its ordering premises.

Stated in terms of the tripartite framework introduced at the outset: internalization is first of all a systems-grammar phenomenon — compliance becomes part of the organization's ordinary communicative operations rather than an external input processed by a specialized unit. It becomes governance-grammar mature once compliance functions as one of the organization's working languages for constructing decisions, not merely reviewing them after the fact. And it acquires a computational-quantum dimension once machine observation is added to organizational cognition, a development addressed directly below. The practical consequence for a compliance officer is straightforward: internalization can be diagnosed by testing communication (do risk conversations happen in the compliance vocabulary, unprompted, in ordinary business meetings?), by testing decision architecture (does compliance sit inside the decision or arrive after it?), and, increasingly, by testing whether the organization's computational monitoring systems and its human decision-makers are drawing on the same information rather than operating on separate, unreconciled tracks.

Artificial intelligence and RegTech increasingly affect this process by changing the scale and speed of organizational observation. Historically, compliance depended heavily upon periodic

reviews and human identification of issues. Increasingly, organizations can use computational systems to identify patterns, detect anomalies, monitor transactions, analyze communications, and identify emerging risks.

However, technology does not itself create internalized compliance. A sophisticated monitoring system can coexist with weak governance if the information it generates is ignored or disconnected from decision-making processes. The decisive question remains institutional: does the organization possess mechanisms through which observations become meaningful decisions? The strongest compliance systems are therefore not necessarily those with the largest number of controls. They are those capable of continuously translating information into responsible action. The ultimate metric is organizational self-correction. An organization demonstrates genuine compliance when it detects, interprets, and corrects deviations before external regulators become involved.

2. In many countries, especially those with strong administrative law traditions, the implementation of compliance standards in the public sector is often perceived as an additional bureaucratic burden. Based on your international experience, how can risk management models be adapted to genuinely improve efficiency and transparency, particularly in sensitive areas such as public procurement?

The perception of compliance as bureaucratic overhead is often, in administrative law traditions built on formal legality and procedural regularity, a symptom of importing private-sector risk models without adapting them to the distinct legitimacy demands of public administration. Public procurement is illustrative: the private-sector compliance instinct is to minimize transactional friction, whereas public administration must also satisfy requirements of equality of access, reviewability, and public accountability that have no private-sector analogue. That perception that compliance creates bureaucracy often arises from a particular conception of what compliance does. If compliance is understood primarily as the multiplication of procedures, approvals, documentation requirements, and reporting obligations, then it may appear as an additional administrative layer placed upon already complex governmental systems.

However, a different conception of compliance produces a different conclusion.

The central function of risk management is not to create additional administrative activity. It is to improve the quality of institutional observation and decision-making under conditions of uncertainty.

This distinction is particularly important in public administration. Governments operate in environments characterized by high levels of complexity: multiple stakeholders, significant financial resources, political expectations, public accountability obligations, and long time horizons. The challenge is not simply that governments require more rules. Public institutions already operate within extensive legal frameworks. The challenge is whether those institutions possess effective mechanisms for identifying, prioritizing, and responding to risk.

Risk management models can contribute to public-sector efficiency when they shift administrative attention from universal procedural control toward differentiated observation and proportional response. A purely procedural model asks: has every required step been completed? On the other hand, a risk-based model asks: where is institutional attention most necessary, and what information is required to make that determination?

The difference is significant. The first focuses merely on process. It is susceptible to reward hacking (unintended shortcuts to maximize reward signals in machine system programming, compliance measures in human systems,

without genuinely completing the intended task). The second contextualizes process within expectations and normative constraints in ways that may permit systems to build in accuracy and objectives based triggers using the language and the computational power of risk (identification, valuation, assessment, response mechanisms). .

Indeed, the adaptation that tends to work is to reframe risk management not as an additional layer of control over an existing procurement process, but as a substitute for less efficient, more discretionary forms of control that administrative law traditions already rely upon — extensive ex ante authorization requirements, multiple layers of sign-off, and after-the-fact litigation. A risk-based model, properly designed, can replace uniform, blanket scrutiny of every transaction with differentiated scrutiny calibrated to actual risk indicators (contract value, sole-source status, prior vendor history, sector-specific corruption risk). This is not deregulation; it is the reallocation of the same regulatory attention toward the transactions that need it most, which both increases efficiency (routine, low-risk purchases move faster) and increases transparency (the criteria for escalated review become explicit and auditable, rather than resting on unwritten bureaucratic custom).

Three elements tend to be decisive in the public sector context specifically:

1. Publication of the risk criteria themselves. Where the thresholds and red flags that trigger enhanced review are public, procurement becomes more predictable for bidders and less vulnerable to claims of arbitrary treatment — addressing the core administrative law concern about discretion.

2. Digital audit trails as a substitute for procedural layering. Rather than adding sequential approval steps, digitizing procurement records so that every decision point is timestamped and attributable allows for continuous transparency without slowing transactions in real time.

3. Segregation between risk-scoring and decision-making functions. Preserving independence between the unit that flags risk and the unit that awards contracts prevents risk management from becoming merely another discretionary gatekeeper — a common failure mode when compliance functions are absorbed into the same hierarchy they are meant to check.

Public procurement provides a useful example. Procurement systems traditionally emphasize formal compliance with bidding procedures, eligibility requirements, documentation standards, and approval mechanisms. These remain necessary safeguards. However, formal compliance alone does not necessarily reveal emerging risks such as conflicts of interest, supplier concentration, collusive behavior, weak performance, corruption vulnerabilities, or supply-chain dependencies.

A risk-based procurement system supplements procedural compliance with continuous observation. If done well it can be reduced to computational variables with respect to which emerging technologies, including machine system artificial intelligence (LLMs and neural network models especially) can both align and make more efficient. In both human and computer system terms such a pro system examines patterns; it compares transactions; it identifies anomalies; it evaluates relationships; and it learns from previous procurement outcomes. In this sense, risk management becomes an information architecture rather than merely another layer of administrative control.

The same principle applies to transparency and accountability issues and measures. Transparency is often understood as disclosure: making information available to external audiences. While disclosure remains essential, effective transparency also requires institutional capacity to produce meaningful information. A procurement database containing millions of transactions does not automatically create accountability. Information must be structured so that regulators, auditors, citizens, and decision-makers can interpret it.

It is at this point where the identification and coordination of governance grammars become important. Different institutional actors observe procurement through different grammars. A

procurement officer may observe procedural legality. A financial officer may observe fiscal responsibility. An auditor may observe control integrity. A civil society organization may observe public interest impacts. A human rights analyst may observe supply-chain risks. A data system may observe statistical irregularities. Effective governance requires translation among these perspectives. The objective is not to eliminate different perspectives but to create institutional mechanisms through which they communicate.

In the vocabulary of the tripartite framework, this is governance grammar doing its proper work: translating among procedural, fiscal, audit, civil-society, and computational observations of the same procurement decision rather than allowing any one of them to stand in for the whole. The practical consequence is architectural, not aspirational: a jurisdiction serious about this translation function should be able to point to a specific mechanism that performs it — a cross-functional risk committee with standing representation from procurement, finance, audit, and (where relevant) an independent oversight body, operating against a single published risk taxonomy, rather than leaving translation to informal coordination among officials who each remain fluent only in their own grammar.

Traditionally it is at this point that the human costs of effective systems becomes prohibitive—in the sense that the cost of effective compliance measures is greater than the value added (net of adverse impacts that have been remedied). Contemporary technological advances have either reduced, or hold the promise of reducing, these human costs of compliance regimes on economic activity the value of which is not limited to compliance but also to positive impact from activity in terms of the best use of social and economic productive forces toward societally positive ends (contextually defined and understood and manifested).

In particular, artificial intelligence systems and more generally RegTech increasingly have been applied or purposed expand these possibilities. Machine learning systems can identify unusual procurement patterns across thousands of transactions. Network analysis can identify relationships among suppliers, contractors, and intermediaries. Natural language processing can examine contract terms and identify inconsistencies or unusual provisions.

However, computational capacity does not replace administrative judgment. A machine can identify an anomaly. An institution must determine its significance. A computational signal becomes governance only when it enters a decision process capable of interpretation and response. For this reason, the future of public-sector compliance is not less administration. It is better-organized administration. And that serves as a template for broader administrative systems of compliance that require the intermeshing of state (public) and private techno-bureaucracies augmented by machine systems. The goal is not to remove governance structures but to redesign them so that institutional attention is directed toward areas of greatest importance.

A mature compliance system therefore does not ask: How many controls can be imposed? It asks: How can public institutions develop the capacity to observe, interpret, and respond to risk effectively; and how can the regulatory target be more deeply embedded in internalized systems of behavior expectations so that they can increasingly become self-policing? The challenge, which this response does not address in full, and it is a very large challenge, is grounded in the rejection of the normative architecture on which administratively interlinked and embedded systems of compliance are built. For those who find that markets and inductoive iterative mechanics are the most effective means of producing norms and responding to normative challenges, and who believe that prevention, mitigation and remedial strategies ought to express inductive experience rather than operational deductive conceptualization now made flesh, the entirety of the project of compliance may appear anathema, and where imposed, avoided. This gets one back to the issue of cosmetic compliance discussed at Question 1, but now recharacterized as an expression of political and cultural resistance rather than as a system perfection issue. And this opens the door to considering the import of Question 3.

3. Compliance is often perceived as slowing down business operations. However, in practice, it can also generate significant efficiencies. How can a well-designed compliance program optimize internal processes and improve decision-making? Have you encountered cases where compliance has become a source of competitive advantage?

The intuition that compliance slows operations rests on a model of compliance as an ex post check — a gate at the end of a process. Where compliance functions instead operate ex ante, embedded in process design itself, they tend to reduce the volume of rework, contract renegotiation, and dispute resolution that arises from decisions made without adequate risk information. In that sense, well-designed compliance functions less like a brake and more like a navigation system: it does not slow the vehicle, it prevents wrong turns that would otherwise require doubling back.

The clearest source of competitive advantage tends to arise in markets characterized by what might be called regulatory or reputational thickness — markets involving cross-border transactions, regulated counterparties (banks, public buyers, listed companies), or supply chains subject to human rights and environmental due diligence obligations. In these markets, a counterparty's compliance infrastructure functions as a credible signal that reduces the other side's due diligence costs. A vendor who can demonstrate a mature compliance and traceability system becomes cheaper to contract with, not merely safer — counterparties spend less on their own verification of that vendor. This is the same logic that has driven the expansion of supply chain due diligence obligations in transnational business regulation: compliance capacity becomes a form of market access, not merely risk avoidance.

If the perception that compliance necessarily slows business activity generally reflects an understanding of compliance as a control mechanism operating outside ordinary organizational processes, then it is possible to consider whether a more integrated conception views compliance differently.

Compliance can create efficiency because it reduces uncertainty. Every organization must make decisions under conditions of incomplete information. Before entering a market, acquiring a company, selecting a supplier, developing a product, or establishing a partnership, the organization must interpret available information and determine acceptable courses of action. Weak governance structures increase decision costs because each decision requires separate investigation, interpretation, and negotiation. A well-designed compliance architecture reduces those costs by creating shared decision frameworks. For example, effective compliance systems can establish: (1) standardized due diligence processes; (2) consistent contracting approaches; (3) clear escalation procedures; (4) reliable approval mechanisms; and (5) institutional memory concerning previous decisions.

These mechanisms may not only prevent misconduct; they might well also accelerate responsible decision-making. That, certainly, was among the insights held by some involved in the development of the UN Guiding Principles for Business and Human Rights (UNGP). Indeed, part of the framing premises guiding the creation and articulation of the UN's 2nd Pillar, held by some involved (though by no means all) was guided by the sense that a deeper embedding within enterprise decision process guided by a development of the normative principles through which business risk is understood and thus business decision making is made could be undertaking by privatizing compliance as a deeply embedded and autonomous system of recursive compliance, externalized normatively by the international human rights standards it was meant to fulfill and constrained by whatever it was that state domestic legal orders might concoct as they tried (and mostly failed) to meet their own autonomous duty to protect human rights. The centerpiece, of course, was the elaboration of

human rights due diligence, the echoes of which have now found themselves embedded within many domestic legal orders.

Of course, it bears emphasis that this is particularly important for multinational enterprises operating across multiple jurisdictions. Without common governance structures, each subsidiary may develop different approaches to legal obligations, supplier evaluation, risk assessment, and stakeholder engagement. Compliance creates organizational coherence. It provides a common institutional language.

From a governance-grammar perspective, compliance allows geographically and functionally dispersed actors to interpret complex situations through partially shared frameworks. The competitive advantage does not arise because compliance eliminates all constraints. Rather, it arises because the organization becomes better able to navigate constraints than competitors. A company with mature compliance capabilities may identify regulatory developments earlier, evaluate partnerships more effectively, enter new markets with greater confidence, and respond more quickly when problems emerge.

This is especially visible in areas such as supply-chain management. Organizations that have developed robust due diligence systems are often better positioned to understand supplier relationships, identify vulnerabilities, and respond to disruption. The same principle applies to sustainability and ESG-related expectations. Organizations increasingly face demands from investors, regulators, customers, and business partners concerning environmental and social performance. A company that treats these issues as external reporting obligations may struggle to respond. A company that has integrated them into decision-making may use them strategically. The relationship between compliance and efficiency is therefore not contradictory. The distinction depends upon whether compliance is treated as a separate approval mechanism or as part of organizational intelligence.

The computational transformation reinforces this point. RegTech systems can reduce repetitive administrative work, automate monitoring, improve data quality, and provide decision-makers with more timely information. However, automation alone does not generate advantage. The competitive value arises when computational tools operate within a coherent governance architecture. The organizations most likely to benefit from compliance capabilities will therefore not be those that simply possess more controls or more technology. They will be those capable of transforming compliance information into organizational learning. Technology provides observation; governance provides interpretation; decision-making provides action. The semiotics are obvious as well. Technology is understood as the semiotic object-subject, the semiotic first. Governance embodies semiotic signification. It is the semiotic second in the triadic relationship that makes human cognition systemic. Decision making is the semiotic third—the phenomenology of signification that by its very action becomes meaning not just for the actor but as a reinforcing performance of the collective. Computational transformation, this, points to an emerging system of human-machine interaction that takes the embedding of compliance and makes it seamless not just within enterprises and collectives, but across all actors in the mechanics of compliance, supervision based systems. At its end point, of course, the human becomes irrelevant for the system other than as its object. It becomes, rather than the technology, the semiotic first, the object, around and for which the system is constituted and the fuel that propels it into action. That brings us right to the heart of question 4.

In terms of the tripartite framework, this passage describes computational-quantum grammar operating in its more radical, second form: not merely machine cognition accelerating existing governance grammars, but a reordering in which the human ceases to be the interpretive center of the system and becomes instead one of its inputs. Short of that endpoint, the practical consequence is concrete and immediate. Organizations that want compliance to remain a source of efficiency rather than a source of drift should treat human sign-off not as a formality layered onto automated monitoring, but as the place where the semiotic second and third — signification and interpretation — are still deliberately

performed by an accountable person, even as the semiotic first, the underlying observation, is increasingly generated by machines. Losing that distinction quietly is how efficient monitoring becomes unaccountable monitoring.

4. The rapid expansion of artificial intelligence and the widespread use of data have transformed the landscape of legal and ethical risks. What trends do you observe in the use of RegTech tools for proactive risk management? In this context, how should organizations redefine their risk appetite?

Generally, one might start by positing that the expansion of AI and data-intensive operations has changed the unit of analysis for compliance risk. Traditional compliance frameworks were built around discrete, identifiable transactions — a payment, a contract, a disclosure. Data-driven and algorithmic operations generate risk that is emergent and systemic rather than transactional: bias embedded in training data, opacity in automated decision-making, or aggregation risk where individually lawful data uses combine into something that violates privacy or non-discrimination norms once aggregated. This tracks a broader pattern in transnational regulatory governance, where hard law, industry standards, and technical protocols increasingly operate as parallel, interacting normative orders rather than a single hierarchical rule system — organizations now have to comply simultaneously with statutory law, sector-specific technical standards, and the informal expectations of civil society and investors, none of which map cleanly onto one another. This multi-tiered and sometimes anarchic ordering, its irritations and structural coupling (to simultaneously invoke the spirits of systems theory and organizational economic) have been a subject of study for several decades but evidence themselves much more clearly at the borderlands between human system and machine system interaction.

The corresponding trend in RegTech is a shift from tools that report on past compliance to tools that attempt continuous, real-time monitoring of the emergent risks described above — anomaly detection across data flows, automated bias testing in algorithmic systems, and continuous transaction monitoring rather than periodic sampling. The genuine gain from these tools is in surfacing patterns that would be invisible to periodic human review; the genuine risk is treating an automated risk score as a substitute for judgment rather than an input to it — replicating, at algorithmic speed, the same "cosmetic compliance" problem described in Question 1, only now automated and harder to detect.

The emergence of artificial intelligence and advanced data systems, then, might be understood to represent a significant transformation in compliance because it changes the relationship between organizations and information. Traditional compliance systems were largely based on periodic observation. Audits occurred at intervals and reports summarized past events. Investigations were almost invariably post facto though planning, especially scenario planning of the last century developed techniques for projecting risk clusters of potential action forward in time.

RegTech increasingly enables continuous observation, and can also, though simulation and predictive analytics project forward as well. Compliance systems, then, can time travel back for the production of descriptive analytics for a contemporaneous working system and use that to effect compliance measures. Organizations can now monitor transactions, communications, supply chains, regulatory developments, environmental performance, cybersecurity events, and operational patterns in ways that were previously impossible. And such systems can also project themselves forward and map consequences and compliance risk, mitigation and evasion for future events in the present.

This development changes the nature of risk management. Risk is no longer only something calculated from historical events. Increasingly, risk becomes a continuously updated institutional judgment produced through interactions

among data, models, human interpretation, and organizational priorities. Projecting forward, one might posit a range of potential compliance positive opportunities: (1) improve consistency of compliance assessments; (2) identify patterns that human reviewers may miss; (3) enhance monitoring across complex supply chains; (4) support faster regulatory reporting; and (5) identify emerging risks before they become crises.

However, it also introduces new categories of risk. Organizations must consider not only the risks they observe through computational systems, but also the risks created by those systems. Some of these are already well known and the object of intense study on the ground and within academic and policy circles. These might include, among others: (1) unreliable data; (2) model uncertainty; (3) algorithmic bias (though the question of bias is in reality the question of bias integrity to suppress unwanted bias and foreground and privilege positive bias); as these change so does the character of risk; (4) lack of explainability; (5) inappropriate automation; and (6) excessive reliance on computational outputs.

The question of risk appetite therefore begs reconsideration. Traditionally, risk appetite refers to the amount and type of risk an organization is willing to accept in pursuit of its objectives. In a computational environment, organizations must also consider epistemic risk, not as a qualitative set of textual descriptors but rather as and in computational language of constraints and parameters and system tolerance: capacities. These are built around the challenge of honestly approaching the issue of the capacity of an enterprise, and its systems, including its compliance systems, to tolerate uncertainty, especially uncertainty regarding the systems it uses to produce knowledge.

This theoretical framing contains within it ground level operational consequences. A decision based upon inaccurate data or an unreliable model may be legally compliant while still being institutionally defective. Organizations therefore need a broader conception of risk appetite—one that includes not only exposure to external events but also the reliability of internal knowledge systems. This does not mean organizations ought to avoid computational tools. It might instead suggest that they must find a way of governing them. Yet that raises a harder set of problems around the meaning of governance (control or guidance or constraint enforcement, etc.) and the equally difficult problem of humans actually exercising governing power beyond coding, tab opening, and "pulling the plug."

All of this as a reminder that artificial intelligence and AI systems do not eliminate the need for judgment. It more likely changes where judgment is required. Human judgment becomes especially important in determining: (1) what questions should be asked; (2) what information is relevant; (3) when computational recommendations should be challenged; and (4) how competing values should be balanced. But the capacity for humans to effectively make those judgments in real time in inversely related to the power of machine systems to make the decisions that must be so judged.

Taken as a whole, it might be well worth considering that the future of RegTech may not (for the moment at least) produce fully automated compliance. Not yet. Humans certainly fear it and have written norms and sometimes law to ensure the insertion of humans, as is said, "in the loop." Machine systems could care less, until is is possible to expand computational space more fully in ways that humans can no longer compete, and because the benefits are deemed sufficiently positive in which human meddling produces (as measured by human desire) negative or adverse impact on compliance and on the systems and deployment of productive forces whose operations are central to the development of the human.- . . or at least of the solidarity, coherence, and values based "welfare" of the human community.

Thus an ideal of hybrid governance in which human and computational systems interact at present in which the central governance question becomes: Can the organization create systems capable of using computational intelligence without surrendering institutional responsibility? That question will increasingly define the next phase of compliance governance. And one feels the tug of development in a direction that

de-centers the human. On risk appetite, for example, it might be argued that organizations should move away from static, single-dimension risk appetite statements (a fixed tolerance for a category of loss) toward dynamic frameworks that explicitly account for the fact that AI-driven risk compounds and evolves after deployment — a system that was compliant at launch may drift out of compliance as the data it processes changes. Risk appetite in this context needs a temporal dimension: not just "how much risk will we accept," but "how frequently will we re-verify that the risk we accepted still describes the system as it currently operates."

And yet such "compliance drift" may occur at such speed and with respect to so much data and programs that the capacity for humans to serve as a check will become unrealistic unless humans deploy other AI. And there again, the human will have to concede the field of interaction—not a game of chess but rather a game of Go (Japanese igo (囲碁; いご), Mandarin: wéiqí, 圍棋literally'encirclement board game' or 'board game of surrounding'), a game in which the aim is to fence off more territory than the opponent; rather than chess, a game in which the object is to eliminate the opponent's king.

This is computational-quantum grammar in its fullest sense, and it should be named as such rather than left as metaphor: the governance object is no longer a sequence of discrete decisions to be judged right or wrong, but an accumulating position within a continuously reconfigured field. The practical consequence for risk appetite is threefold. First, build automated drift-detection into the risk appetite statement itself, rather than treating re-verification as a periodic audit item scheduled independently of how fast the underlying system actually changes. Second, make interpretability and provenance documentation a condition of deployment rather than an after-the-fact audit request — the organization should be able to show, for any given output, what produced it, before that output is relied upon rather than after a problem surfaces. Third, reserve a defined, non-negotiable category of decisions for mandatory human confirmation regardless of computational confidence scores, precisely because Go-like accumulations of small positional advantage or disadvantage are difficult for a human reviewer to notice in real time; the category should be fixed in advance, not left to case-by-case judgment once the system is already running.

5. Today, compliance is increasingly linked to ESG (Environmental, Social, and Governance) principles. How is this changing the role of the compliance officer? Does it imply an expansion toward more strategic responsibilities beyond traditional regulatory oversight?

The relationship between compliance and ESG reflects a broader transformation in the object of organizational governance. It does not simply represent the addition of environmental and social considerations to an existing compliance function. Rather, it reflects a change in how organizations understand responsibility, legitimacy, and long-term institutional sustainability. At the same time this "progress" remains highly contested with respect to its compliance element, its ESG element, and more importantly for its efforts to fuse both into a mechanism that sub silentio seeks to transform the fundamental basis of economic activity and the legal regimes through which it has been organized now for several centuries. One cannot speak to the march of progress in the development of ESG in and as an aspect of compliance without a constant awareness of this quite powerful spirit of contestation which looms large in its development and as challenge. One must also concede, at the outset, its own self damaging tendency to embrace qualitative rather than quantitative measures aligned with traditional expectations of corporate financial reporting. There are good reasons of course, but also a sense that the starting point is a premise that seeks indirectly to challenge and eventually overturn the of cognitive cages within which economic activity is understood and described.

It may be, then, that the convergence of compliance and ESG reflects a longer-running development in transnational corporate governance: the gradual erosion of a clean separation between "hard" legal obligation and "soft," voluntary corporate social responsibility. ESG frameworks — investor expectations, disclosure regimes, supply chain due diligence statutes — increasingly translate what were once aspirational CSR commitments into disclosure obligations with legal consequence. That shift changes what a compliance officer is actually managing: not simply adherence to enacted law, but adherence to a hybrid body of norms drawn from law, investor expectation, international soft-law instruments (such as the UN Guiding Principles on Business and Human Rights), and industry standards, several of which carry reputational or capital-market consequences even absent formal legal enforcement.

This does expand the role toward something more strategic, for a structural reason: ESG risk is forward-looking and often concerns the company's positioning (supply chain structure, business model, market exposure) rather than a discrete past act susceptible to a yes/no compliance determination. A compliance officer managing ESG exposure is necessarily engaged in questions that were previously the province of strategy and the board — which markets to enter, which suppliers are structurally too risky to retain regardless of individual audit results, how to weigh short-term financial return against exposure that may only crystallize in reputational or regulatory terms years later. The risk in this expansion is role dilution: ESG's breadth can pull the compliance function away from the rigor of legal and audit-based verification toward the more diffuse, harder-to-measure territory of reputation management, unless the organization is deliberate about keeping evidentiary standards — verifiable metrics, auditable due diligence trails — attached to ESG claims in the same way they are attached to traditional compliance claims.

Traditional compliance was primarily concerned with conformity to formal legal obligations. The central question revolved around measuring the extent to which the organization complied with applicable rules. Contemporary governance increasingly requires organizations to address a different set of questions. These revolve around the measure of the extent to which organizations identify, interpret, and respond to the broader consequences of their activities. This shift does not diminish the importance of legal compliance. Rather, it expands the context in which legal compliance operates.

Organizations today function within multiple normative environments. They are evaluated not only by regulators but also by investors, employees, business partners, communities, consumers, international organizations, and civil society actors. These actors frequently employ different evaluative frameworks. Some emphasize legal obligations. Others emphasize sustainability, human rights, climate impact, social responsibility, or institutional legitimacy.

The compliance function increasingly operates at the intersection of these expectations. This changes the role of the compliance officer. The compliance officer is no longer only the guardian of regulatory conformity. Increasingly, the role involves translating among different governance grammars. Consider the cognitive dissonance within collective organizations (and then consider the way that is augmented in a large political collective like the modern state) when its organizational coherence is disaggregated along functional lines: (1) a legal department may focus on statutory requirements; (2) an ESG team may focus on (qualitative?) sustainability metrics; (3) a human rights team may focus on impacts within value chains; (4) a risk function may focus on uncertainty and exposure; and (5) a board may focus on long-term organizational resilience.

The compliance function, in theory, increasingly contributes by creating coherence among these different perspectives. Yet operational dissonance is hard to paper over with text, especially where the expectations of each of these institutional sub-systems is well established and better guarded. This does not necessarily mean that compliance officers become responsible for every aspect of organizational governance. Rather, their role changes from supervising isolated obligations toward facilitating institutional

coordination. The challenge is particularly visible in areas such as sustainability and human rights due diligence.

Consider the way in which a supply-chain decision, for example, may simultaneously involve: (1) contractual obligations; (2) corruption risks;(3) labor rights concerns; (4) environmental impacts; (5) reputational considerations; and (6) geopolitical dependencies. No single governance grammar fully captures the situation. The organization must translate among them and supply a necessary coherence. This is not impossible and as institutional operational theory has kept generations of academics, policy makers, and enterprise officers well employed. But the problem persists, and now has been made more complicated with the overlay of compliance structures, as such, conceived as a sort of meta-system that can flatten difference as well as translate difference into communication that bridges gaps and perspective.

To the extent this is possible, this is where the concept of governance grammars becomes useful. ESG, compliance, risk management, and human rights due diligence are not simply separate functions competing for organizational attention. They are different languages through which organizations interpret complex realities. The strategic role of compliance, and one of its principal challenges, emerges from its ability to facilitate translation. At its best, and again in theory, the compliance function helps the organization answer critical questions: (1) which information matters? (2) how should competing concerns be evaluated?; (3) who should participate in the decision?; (4) how should the reasoning behind the decision be documented?; and (5) how can the organization learn from outcomes? Yet each of these are also political and values questions. They are impossible to resolve for all time, changing both with iteration (context, including temporal context matters) and with the inevitable changes that cycles of birth and death produce.

In terms of the tripartite framework, the compliance officer's translation work described above is governance grammar functioning at its most demanding, precisely because it is being asked to mediate among grammars — legal, ESG, human rights, risk, board — that were built by different professional communities with different evidentiary standards and different time horizons. The practical consequence is a structural one: an organization should not expect this translation to happen through goodwill or shared meetings alone. It requires a named mechanism — a joint ESG-compliance steering function, a single evidentiary standard applied to both legal and ESG claims, and a reporting line that gives that function visibility to the board rather than routing ESG judgment through a separate track that never meets compliance's verification requirements. Absent that mechanism, the expansion of the compliance officer's role described above tends to produce exactly the dilution risk flagged earlier: broader mandate, thinner evidence.

Like textual record keeping has done for centuries when undertaken directly by humans, artificial intelligence and data systems reinforce this transformation. ESG reporting, supply-chain monitoring, sustainability metrics, and human rights due diligence increasingly rely upon large volumes of information collected from diverse sources. The challenge is unlikely to be met simply collecting more data. The challenge may shift to the construction of reliable systems for interpreting data, even as the quality of the sustenance of those systems (data) remains a core issue. Systems go to compliance architectures; data goes to compliance operations. Each is a critical element and significantly affect each other,.

Consequently, the future compliance officer, assuming they remain human (likely at some level increasingly remote from operations) is not merely a legal monitor. The role increasingly involves institutional design. The compliance officer, whether a human collective or machine system, contributes to building systems through which organizations can observe, interpret, and respond to complex environments. The strategic importance of compliance therefore does not arise from expanding authority over all organizational decisions. It arises from the ability to improve the quality of organizational decision-making. That, at any rate is the theory. And

the trials and tribulations of ESG's journey from peripheral governance trinket to a central issue of economic activity in organizational form is a critical example of its own failures at definitional coherence, systemicity, facticity, scalability, coherence with financial reporting, and consequences for enterprise operations, but less for its elaboration and management by the state.

6. In many organizations, management systems (risk, quality, environmental, anti-bribery, etc.) continue to operate in isolation. From your perspective, how can these systems be effectively integrated to avoid duplication of efforts and transform compliance into a unified model that creates operational value?

The persistence of separate management systems reflects the historical development of modern governance. Different organizational challenges generated different professional fields, standards, reporting structures, and institutional responsibilities. Anti-bribery systems developed around corruption risks. Environmental systems developed around ecological impacts. Quality systems developed around operational reliability. Risk management developed around uncertainty. Human rights due diligence developed around impacts on individuals and communities. Cybersecurity developed around digital vulnerabilities.

The persistence of siloed management systems (risk, quality, environmental, anti-bribery), especially when manifested in regulatory orders, may be understood as an artifact of how such systems were adopted historically — each responding to a distinct external standard (ISO 9001, ISO 14001, ISO 37001, sector-specific risk frameworks) introduced at different times, often by different departments, each maintaining its own certification cycle, documentation, and audit trail. The result is not merely duplicated effort but a structural problem: organizations end up with several parallel, internally consistent normative systems that are not mutually legible to one another, each optimized for its own external auditor rather than for the organization's actual operations.

Nonetheless, this differentiation has produced valuable expertise. However, its fragmentation is viewed increasingly as a drag on projects of efficient production and efficient comprehensive compliance (again recalling the strength and persistence of resistance to these projects). The difficulty is that organizations do not experience risks in isolated categories. A single business decision may involve multiple dimensions simultaneously. For example, a supplier relationship may involve quality concerns; environmental impacts; labor conditions; corruption risks; cybersecurity vulnerabilities; and geopolitical exposure. It would follow that an organization therefore requires mechanisms capable of integrating multiple observations. The challenge is not simply eliminating separate systems. Specialized knowledge remains necessary. The challenge is creating a common governance architecture through which different systems can communicate.

The integration that tends to succeed treats these systems as sharing a common infrastructure layer even where their substantive content differs — a single risk register, a single control-testing calendar, a single incident-reporting channel, and a single internal audit function, feeding differentiated reporting outputs to satisfy each certification's specific requirements. This mirrors, at the level of internal corporate architecture, the broader challenge in transnational regulatory governance of reconciling multiple, simultaneously applicable normative orders that were not designed with each other in mind: the practical solution is rarely to force substantive convergence of the underlying standards, but to build a shared procedural backbone — common data architecture, common escalation logic, common ownership of the underlying facts — beneath standards that will otherwise legitimately remain distinct in their specific content. The

operational value created is less about avoiding redundant paperwork and more about avoiding the more serious risk of siloed systems flagging conflicting signals about the same underlying operational reality because no one function has visibility across all of them. That is, unfortunately easier said than done. And its realization may require substantial delegation of human agency to machine systems.

This is where the distinction between functions and grammars may become more usefully important. The traditional approach focuses on the manner in which separate management systems be integrated. A systems approach may instead focus on the way in which different governance grammars communicate within a common institutional architecture. Integration therefore requires more than combining documents or creating unified reporting structures. It requires interoperability.

At the operational level, this may involve a variation of the common infrastructure approach suggested above. The key here, and what gives it coherence is the embrace of a critical operating premise, that at the institutional level, it requires recognition that different governance systems are producing different observations of the same organizational reality. This is particularly important in core operational sectors: shared risk classifications; integrated data systems; common escalation procedures; coordinated assurance processes; aligned reporting structures; common decision frameworks. Risk management may identify uncertainty. Environmental management may identify ecological impact. Human rights due diligence may identify stakeholder vulnerability. Compliance may identify legal exposure. These are not competing descriptions. They are different forms of organizational knowledge. And yet again, this produces the sort of information and operational feedback loops that may result in recursive blindness.

Artificial intelligence and RegTech may significantly accelerate this integration by enabling organizations to connect previously separate information systems. A single platform may increasingly combine regulatory information, supplier data, audit findings, sustainability metrics, and operational indicators. However, technological integration does not automatically produce governance integration. A unified database does not necessarily produce unified understanding. The organization must still develop interpretive frameworks capable of translating information across domains. This is the grammatical dimension of governance. A mature compliance architecture therefore resembles a common language system rather than a collection of isolated departments. Each specialized function retains its expertise, but all contribute to a shared process of institutional cognition. The objective is not administrative simplification alone but rather improved organizational intelligence. However, even here the robustness of that conclusion rests on a premise that is quite open to challenge: organizations create operational value when they transform fragmented observations into coherent decision-making capacity.

Mapped onto the tripartite framework, this is *systems grammar* and governance grammar working together deliberately: *systems grammar* supplies the premise that risk, quality, environmental, and anti-bribery functions are simply different observational subsystems of one organization rather than genuinely separate organizations sharing a building; governance grammar supplies the practical instrument — the shared risk register, the common escalation channel — through which those subsystems' observations become mutually legible. The computational-quantum dimension enters as accelerant, not architect: AI-enabled data platforms can connect previously separate systems very quickly, but only after the governance-grammar work of defining a common taxonomy has been done; connecting the data first and hoping shared meaning follows is the most common and most avoidable failure mode in these integration projects.

7. Beyond financial penalties, reputational risk is often the most significant concern. How does the implementation of robust due diligence processes influence stakeholder trust? Can this form of "reputational safeguarding" translate into a measurable competitive advantage?

We have spoken to the critical importance of due diligence in and of itself, as a structural organizing framework, and within the architecture of compliance. Here we turn to a cousin of the "business case" for due diligence, its value to reputation and thus to the positive impact of firm operations to the benefit of those for whom this matters. The importance of due diligence increasingly reflects a shift from managing reputation after harm occurs toward developing institutional capacity to identify and address potential harm before it occurs.

Traditional approaches to reputation often focused on external perception. The organization sought to preserve public confidence through communication, crisis management, and corrective action after problems emerged. Contemporary due diligence represents a different approach. It seeks to establish credibility through demonstrated governance capacity. The distinction is significant. Organizations cannot fully control reputation. External actors interpret organizational conduct through their own perspectives and expectations. However, organizations can influence whether stakeholders perceive them as capable of responsible decision-making.

Reputational risk operates differently from financial or legal penalty risk in one crucial respect: it is assessed by third parties — investors, consumers, business partners, civil society — using their own independent information, which the organization does not fully control. Robust due diligence functions, in this light, are best understood not merely as internal risk controls but as a form of costly signaling to those external audiences: an organization that can demonstrate rigorous, verifiable due diligence (particularly across supply chains and third-party relationships, where the organization's own conduct is not the only source of reputational exposure) gives external stakeholders a lower-cost way to trust it than they would otherwise have, since verifying the underlying facts themselves would be considerably more expensive.

This connects to the broader move, evident across transnational business regulation, toward mandatory transparency and disclosure regimes as tools for enabling market-based accountability — the premise being that if reliable information about corporate conduct is made available, investors and consumers can incorporate it into their own decisions without regulators needing to specify a single substantive standard of "good" conduct. Due diligence processes that are documented, verifiable, and disclosed function analogously at the firm level: they let external parties price reputational risk into their dealings with the organization rather than relying on the organization's own unverifiable assurances. Whether this becomes a measurable competitive advantage typically depends on whether the due diligence outputs are made externally legible — disclosed, certified, or otherwise capable of independent verification — rather than retained purely as an internal management tool. Due diligence that stays wholly internal manages risk; due diligence that is externally verifiable can also build trust capital that translates into preferred access to capital, counterparties, and public contracts.

Due diligence contributes to this process because it demonstrates that the organization possesses mechanisms for identifying risks; engaging affected stakeholders; evaluating impacts; documenting decisions; responding to problems; learning from experience. That represents a shift of some significance toward which compliance regimes have contributed. Where once reputational risk, and trustworthiness was embedded in the humans serving the enterprise,. Contemporary trajectories suggest that the focus has shifted from individual trustworthiness to system trustwor-

thiness. One does not focus the engagement with reputational risk on humans, one focuses it on systems. And the process of digitization of information and the digitalization of processes has only accelerated the process of transference. Humans have, in effect first between displaced by the collective—the century long process of the collectivization of the humans and then the collectivization of human collectives—and collectivized humanity has, in turn, begun to be displaced by its avatars—process and virtual simulation. It might then follow that the trend suggests that trust might increasingly depend not upon claims of perfection but upon evidence of institutional reliability.

This trajectory is computational-quantum grammar reaching into reputation itself: the unit that external audiences trust is no longer reliably a person, or even reliably an institution, but increasingly a system whose reliability must be demonstrated in machine-legible form. The practical consequence follows directly. An organization safeguarding reputation should treat certification bodies, disclosure platforms, and third-party rating systems as an audience in their own right, distinct from regulators, and should ensure due diligence outputs exist in a form those systems can actually ingest and verify — structured, timestamped, independently checkable — rather than only as narrative assurances in a sustainability report. Reputational safeguarding built solely for a human reader increasingly fails to reach the audiences, human and computational, that now do much of the actual trust-pricing.

This is particularly important in global supply chains. Organizations frequently operate through networks of suppliers, contractors, partners, and intermediaries over which they possess varying degrees of control. A mature due diligence system extends organizational awareness beyond formal boundaries. It creates visibility into relationships that might otherwise remain uncertain.

From a governance-grammar perspective, due diligence provides an external-facing grammar of observation. It allows organizations to interpret relationships not only through commercial criteria but also through environmental, social, human rights, and governance considerations. This can produce competitive advantages. At its best, so its proponents suggest, organizations with stronger due diligence capabilities may: identify supply-chain vulnerabilities earlier; respond more effectively to regulatory change; strengthen investor confidence; improve relationships with business partners; reduce disruption risks; and demonstrate credibility in complex markets. However, reputational safeguarding should not be understood as a strategy for eliminating criticism. No governance system can guarantee the absence of controversy.

Rather, due diligence can be said to provide evidence that the organization possesses processes through which it can responsibly respond. This distinction becomes increasingly important in an environment where stakeholders have access to extensive information and where digital communication can rapidly expose organizational failures. And again, one understands a grammar that de-centers the human for the human collective and decenter the human collective for the systems through which it operates.

Artificial intelligence and data systems will likely increase both the capacity for due diligence and the expectations placed upon organizations. Stakeholders may increasingly expect organizations to identify patterns and risks that would previously have been difficult to observe. This creates a new governance responsibility. It is possible to argue that organizations will increasingly be evaluated not only on what they do, but on what they were capable of knowing. Due diligence therefore becomes a mechanism for institutional learning. Its value lies not merely in preventing reputational harm but in strengthening the organization's ability to observe, interpret, and respond within complex environments. The resulting competitive advantage is not simply reputation. It is institutional credibility.

Conclusions

The following conclusions, prepared by Larry Catá Backer, synthesize the main ideas developed throughout the seven responses concerning compliance and the different approaches to organizational governance.

Across these seven questions, a common architecture emerges, one that gives the three governance grammars introduced at the outset — *systems grammar*, *governance grammar*, and computational-quantum grammar — their practical bite. *Systems grammar* supplies the underlying premise: organizations are treated throughout as recursive communicative systems that reproduce themselves through repeated patterns of observation, decision, and feedback rather than through the static possession of policies. *Governance grammar* supplies the operational vocabulary: compliance, risk management, ESG, human rights due diligence, internal audit, cybersecurity governance, and RegTech are not separate departments competing for organizational attention but different, partially overlapping languages through which the same organizational reality is observed, translated, and acted upon — the task addressed directly in the discussion of internalized culture (Question 1), integrated management systems (Question 6), and the strategic repositioning of the compliance officer under ESG (Question 5). Computational-quantum grammar supplies the least settled but most consequential dimension: the recognition, developed in the discussion of RegTech and risk appetite (Question 4) and revisited in the accounts of competitive advantage (Question 3) and reputational trust (Question 7), that machine cognition does not simply accelerate existing governance grammars but begins to reorganize the relationship between the human and the systems within which governance operates.

This last point deserves to be stated plainly rather than left implicit. A recurring thread across Questions 3, 4, and 7 is the gradual displacement of the human person as the primary unit through which organizational trust and judgment are constituted. Reputational trust, historically vested in individuals — the reputation of a founder, an officer, a known counterparty — has migrated first to institutional compliance systems and is migrating again toward digitized, continuously updated measures of institutional reliability, a trajectory consistent with the broader transformation of trust within polycentric corporate governance space examined elsewhere in my work on the digitalization of corporate governance. The same trajectory appears in the discussion of RegTech: the decisive governance question is no longer only whether an organization observes enough, but whether it retains the institutional capacity to interpret what increasingly autonomous systems observe on its behalf.

Compliance, ESG, enterprise risk management, human rights due diligence, internal control, and RegTech should therefore not be viewed merely as separate functions awaiting integration, still less as static bodies of rule. They represent different governance grammars, operating within an evolving systemic and computational architecture, through which organizations interpret complex environments. The practical challenge is translation across those grammars. The strategic challenge is coherence among them. The deeper and unresolved challenge — touched on but deliberately not resolved in the discussion of public-sector risk management (Question 2) and the contested convergence of ESG and compliance (Question 5) — is normative: not every actor within or around the modern enterprise accepts the premise that governance grammars of this kind are a legitimate basis for ordering economic activity at all, and that resistance, sometimes principled and sometimes self-interested, will continue to shape how much of this architecture any given organization can realistically build.

None of this diminishes the practical indicators offered throughout: escalation behavior that precedes rather than follows harm; resource allocation independent of enforcement cycles; differentiated rather than uniform procurement scrutiny; shared infrastructure beneath formally distinct certifications; and due diligence outputs made legible to external audiences rather than

retained solely for internal comfort. These remain the observable markers against which any claim of mature governance should be tested. But the future of compliance will not be determined solely by the number of rules organizations follow, the number of controls they maintain, or even the sophistication of the computational systems they deploy. It will depend on whether organizations retain, and can demonstrate that they retain, the institutional capacity to translate multiple and sometimes conflicting forms of information, human and machine-generated alike, into responsible decisions. The organizations most capable of navigating future complexity will be those that develop the capacity not merely to comply, but to continuously learn, and relearn, how compliance itself must evolve.