Deloitte.

Compliance Engineering:
Navigating the Future of Digital Trust and Innovation

March 2025

Imagine this...

A leading application developer (company), a trailblazer in the digital media industry, was preparing to launch a groundbreaking, culture-shifting application after months of rigorous planning, development, testing, and marketing. All signs pointed to a successful on-time release, but just weeks before the scheduled launch, a last-minute review revealed several compliance gaps that could negatively impact the product's security and user safety.

The company decided to accept several low-grade security risks and push the development of required functionalities to the next release. The product launched on time, and user engagement exceeded its performance targets and Wall Street expectations. However, a week later, activist hackers (hacktivists) exploited low-grade security vulnerabilities and exposed the private details and communications of high-profile public figures within the application. As a result, an investigation was launched by several regulators resulting in multiple fines for non-compliance while the victims of the hack filed a lawsuit against the company. The company's stock price plummeted, forcing it to roll back the application causing delays in the launch of road-mapped companion products.

The scrutiny, pressure, and business impact on the company could have been prevented. Imagine if the company's product development tools provided compliance prompts and tips while engineers were designing their products; imagine if these engineers were assisted by agentic artificial intelligence (AI) or agents that provide compliant code and features that significantly reduce risk and help enable compliance with regulatory requirements; and imagine if the company also operated risk review processes that evaluated and addressed privacy, security, safety, and digital ethics product risks prior to launch. We refer to this practice as **Compliance Engineering**. The practice of Compliance Engineering not only proactively reduces potential risks and enables compliance, but also allows organizations to establish trust with users, shareholders, and regulators more effectively.

In the rapidly evolving technology age, where innovation and time-to-market are critical drivers, compliance is essential to staying competitive. As organizations push boundaries to outpace competitors, adhering to regulations is not just advantageous—it's crucial. Compliance Engineering promotes the development and release of trustworthy experiences, products, and services while avoiding unnecessary costs associated with fines, lawsuits, product roll backs, and launch delays.

The Case For Change

Faced with an accelerating pace of regulatory change and an even faster evolving competitive and user landscape, achieving compliance can feel like trying to hit a moving target. However, this is still attainable by putting customers and users first and executing engineering strategies aimed at building trust in addition to engagement. Compliance Engineering is not just becoming a business imperative but also a critical response to evolving customer expectations, expanding regulatory obligations, increasing competition, and rising cost pressures.

Customer Expectations

Customers are no longer satisfied with just the core functionality of a product. Now, they care about the protection of their privacy and the safety of the product, demanding more transparency from organizations. Customers expect experiences, products, and services to be developed with effective guardrails to protect them against harm, including fraud, theft, and personal data misuse.

Changing Customer Sentiment: Customer sentiment has shifted from wanting to be in control to actually "feeling" in control over how they engage with the product or service. This means organizations should embed privacy, security, and trust practices into the product or service, and clearly inform customers up-front about why their data might be collected, what it may be used for, and how their experience may be enhanced or impacted as a result. Additionally, customers want confirmation that their engagement with the product or service will be secure and protected from harm or abuse.

Loyalty and Engagement: Trust in a product or service has become a driver of customer engagement and loyalty. Reports indicate that 75% of consumers who highly trust a brand are likely to try the brand's new products and services, suggesting that trust not only retains customers, but also encourages them to explore additional offerings from the brand.[1] In fact, trusted brands have been found to outperform low-trusted competitors by up to four times more in terms of total market value.[2] Customers are even showing willingness to pay a premium for their business. Internally within organizations, 94% of global boards believe building trust is important to the organization's performance, with 83% of global boards believing that action is needed within 6 months.[3]

Regulatory Obligations

The current digital regulatory environment is continuously evolving, becoming both expansive and specific, with higher penalties for non-compliance. This dynamic regulatory growth adds complexity for organizations striving to maintain compliance while operating globally.

Expanding Scope and Specificity: Based on recent data, 71% of countries have data protection and privacy laws in place, while an additional 9% have draft legislation.[4] As of April 2024, more than 300 AI-related laws, guidance, or regulations have passed or are in development across the globe.[5] Furthermore, regulatory bodies expect organizations to make substantial efforts to evidence their adherence to the expanding scope of compliance regulations. These regulations have consequences that extend beyond mere legal compliance, with organizations facing requests for information, investigations and inquiries, enforcement actions, and even requests for data deletion. The bare minimum is no longer simply responding to regulatory

1 Source: Deloitte, "Navigating Trust: An Advertiser's and Marketer's Guide to Data, Privacy, and Trust", https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Advisory/us-advisory-navigating-trust.pdf

2 Source: Ashley Reichheld & Amelia Dunlop, as cited in Deloitte, "The Four Factors of Trust", https://www2.deloitte.com/us/en/pages/about-deloitte/solutions/four-factors-of-trust.html

3 Source: Deloitte, "The Importance of Enterprise Trust", https://www2.deloitte.com/us/en/pages/advisory/solutions/the-importance-of-trust-in-your-organization.html

4 Source: Deloitte, "Consent & preference management (CPM) Point of View", https://kx.deloitte/documents/view/82763?u=1

5 Source: Deloitte, "AI risk and approaches to global regulatory compliance" https://www.deloitte.com/uk/en/Industries/technology/perspectives/ai-risk-and-approaches-to-global-regulatory-compliance.html

requests – companies are now required to demonstrate compliance proactively, including detecting vulnerabilities and designing products with compliance in mind before an incident occurs.

Nuanced and Specific Regulations: Regulations are becoming increasingly nuanced and varied across industries and geographies. For example, the Digital Fairness Act in the European Union seeks to regulate the addictive design of digital products and marketing by social media influencers. It is equally important that organizations prepare their teams and workflows to assess compliance against smaller requirements as well. A compliance function that systematically evaluates its products and processes to address frequent regulatory changes is better positioned to maintain a competitive edge and achieve sustained success.

Competition

The relentless drive to innovate faster, be the first to market, and build better products has intensified in recent years. This attitude has heightened competition and put immense pressure on compliance teams, which need to manage a broader range of factors and potential risks without slowing down product engineering teams.

Navigating Complex Technologies: With the introduction of complex technologies such as Generative AI (GenAI), engineering and compliance functions need to navigate issues related to data privacy, ethical AI use, cybersecurity, and intellectual property. The sheer volume and complexity of these product launches, combined with evolving regulations, can overwhelm traditional compliance processes, making it difficult for organizations to launch competitive products quickly without creating user or compliance risks.

Competitive Advantage through Compliance: Building strong compliance programs and engineering practices can drive financial returns, operational efficiencies, and competitive advantages. A 2020 study found that more than 70% of organizations reported significant business benefits from investing in privacy beyond mere compliance.[6] These advantages include enhanced agility, increased competitive differentiation, improved investor appeal, and heightened customer trust. The same study revealed that organizations, on average, receive benefits equating to 2.7 times their investment in privacy initiatives.

Cost Pressures

Non-compliance can lead to significant financial repercussions. However, the compliance cost is ballooning across sectors due to the proliferation of regulations and novel online threats. This dual pressure of rising compliance costs and the need to reduce spending has compelled organizations to increase efficiencies by adopting an innovative, technology-first approach to Compliance Engineering.

Efficiency and Cost Cutting: Organizations, specifically in the technology sector, are under significant pressure to enhance efficiency and reduce costs driven by economic challenges, technological advancement, and competitive dynamics. A Q4 2023 Deloitte survey of 122 executives revealed that the top organizational priority is efficiency, with innovation and productivity as close runner-ups.[7] For many organizations, these cost cuts are necessary for big investments in new businesses and AI.

Rising Compliance Costs: The cost of compliance is escalating, largely due to the increasing number of regulations and the expanding scope of products and services. These costs can strain budgets and divert funds that could be used for innovation and research and development (R&D). Around 50% of engineering is spent on fixing bugs.[8] However, investing in Compliance Engineering capabilities will allow engineers to avoid bugs, reduce time spent fixing them, and streamline the build of launch-ready products. Furthermore, a study highlighted that while the average cost of compliance is approximately $5.47 million, the cost of non-compliance is around $14.82 million – nearly 3x higher than compliance costs.[9]

6 Source: Cisco Systems, "Cisco 2020 Data Privacy Benchmark Study Confirms Positive Financial Benefits of Strong Corporate Data Privacy Practices", https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2020/m01/cisco-2020-data-privacy-benchmark-study-confirms-positive-financial-benefits-of-strong-corporate-data-privacy-practices.html

7 Source: Deloitte, "2024 technology industry outlook", https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/2024-tmt-outlook-technology.pdf

8 Source: Deloitte, "DevOps, SRE, and the reliability life cycle", https://www2.deloitte.com/us/en/blog/deloitte-on-cloud-blog/2023/devops-SRE-reliability-lifecycle.html

9 Source: GlobalSCAPE; Ponemon, "The Trust Cost of Compliance with Data Protection Regulations", https://static.fortra.com/globalscape/pdfs/guides/gs-true-cost-of-compliance-data-protection-regulations-gd.pdf

Enabling Digital Trust Through Compliance Engineering

The Importance of Trust

Digital Trust is the earned confidence and reliance on a digital platform, product, or service by its consumers. While trust has always been essential, it is now a crucial currency that organizations use to engage with customers in exchange for their business and loyalty, especially as organizations become more digitally integrated.[10] In addition to customers, trust has become essential in the organization's ability to build positive relationships with regulators, employees and their boards, and the public. However, many organizations are still struggling to achieve trust from their breadth of stakeholders. This issue is further complicated by the rapid digital transformation efforts occurring in many industries, which tap into newer and more sensitive ways organizations are connecting with their customers, such as personal information and online behavior. It's important for organizations to remember that trust is a currency that takes a long time to earn but can easily be erased or broken.

Engineering Trusted Products

While there isn't a silver bullet to solve the trust dilemma, there are interdisciplinary practices across technology and processes that can help. Typically, organizations are familiar with using security, privacy, safety, and compliance by design practices to support regulatory readiness. Security teams generally have implemented well-established technical practices including threat modeling, static code review, dynamic code review, and penetration testing. There are accepted technical ways to troubleshoot product issues and test whether they are susceptible to cyberattacks. At each stage of the development life cycle, leading organizations are testing their products from a security and privacy perspective.[11]

Compliance Engineering aims to fuse these 'by design' practices, collectively known as "trust by design", and enhance their effectiveness by leveraging AI and other leading technology to systemically address organizational risks and protect customers. Features associated with Compliance Engineering include but are not limited to:

- Integrated risk review processes or "trust by design"
- Reusable trusted code repository that house policies translated into code
- Dynamic compliance prompts and tips offered to engineers as they advance through the product development lifecycle
- Compliance and risk agents that provide real-time feedback and support during coding and development
- Empowered engineers that build with compliance in mind

Furthermore, many organizations strive to design, build, and launch secure and trusted digital platforms, products, and services that align with customer and regulatory expectations. When outcomes fall short of these expectations, products may not be optimal, companies may struggle to use them, and engineers may need to revisit initial design steps to address the issues, recode, and incorporate the necessary considerations. This process can increase costs and extend the time to market.[12]

10 Source: Deloitte, "Digital Trust Maturity Survey", https://www.deloitte.com/global/en/services/consulting-risk/perspectives/earning-and-building-greater-digital-trust-through-cyber.html

11 Source: The Wall Street Journal & Deloitte, "Trust by Design: A Path to Inclusive, Compliant, Safe Products", https://deloitte.wsj.com/cio/trust-by-design-a-path-to-inclusive-compliant-safe-products-3a6827a2

12 Source: The Wall Street Journal & Deloitte, "Trust by Design: A Path to Inclusive, Compliant, Safe Products", https://deloitte.wsj.com/cio/trust-by-design-a-path-to-inclusive-compliant-safe-products-3a6827a2

Measuring Trust in a Digital Product

Digital trust can be measured as a function of several key factors, each contributing to the overall trust level within an organization. The equation can be represented as:

Digital Trust = f(Privacy, Transparency, Safety, Compliance, User Experience, Security)

```
>> # Digital Trust
>>
>> # Define Weights for each factor
>> w1 = 0.2
>> w2 = 0.15
>> w3 = 0.25
>> w4 = 0.1
>> w5 = 0.2
>> w6 = 0.1
>>
>> # Define the function for Digital Trust
>> def calculate_digital_trust (P,T,SA,C,U,S)
>> return (w1*P) + (w2 * T) + (w3 * SA) + (w4 * C) + (w5 * U) + (w6 * S)
>>
>> #Example Values for each Factor
>> Privacy = 8
>> Transpareny = 7
>> Safety = 9
>> Compliance = 6
>> User_Experience = 8
>> Security = 7
>>
>> #Caculate Digital Trust
>> digital_trust = calculate_digial_trust(Privacy,Transpareny, Safety, Compliance,User_Experience, Security)
>> print("Digital Trust Score:", digital_trust)
>>
```

Each factor in the digital trust equation can be defined as follows:

- **Privacy:** Reflects the organization's commitment to protecting user data and respecting user privacy.
- **Transparency:** Indicates how openly the organization communicates its practices, policies, and any incidents that occur.
- **Safety:** Reflects the organization's commitment to prevent abusive behavior and content, bias, copyright infringement, and discrimination.
- **Compliance:** Adherence to relevant laws, regulations, and industry standards.
- **User Experience:** Encompasses the overall usability, accessibility, and satisfaction of the users interacting with the organization's digital platforms.
- **Security:** Measures the robustness of an organization's defenses against cyber threats and data breaches.

These factors are not all evenly weighted, which means when one factor is prioritized over another factor, it has implications for the others. Therefore, a combination of these six factors is important to cementing digital trust.

To maintain and enhance digital trust, organizations should proactively manage these risks, engage transparently with consumers, and commit to ethical data practices. Balancing these pressures involves continuous improvement, proactive risk management, and clear accountability. By addressing these challenges effectively, organizations can foster strong, lasting relationships with their stakeholders and build a resilient trust framework.

Activating Compliance Engineering

Since the dotcom era, through the rise of social media and digital advertising, to today's focus on cloud computing, the Internet of Things (IoT), and AI and machine learning (ML), consumer trust has driven organizational growth and innovation. The proliferation of user generated content and AI complicates distinguishing real from fake content, making it pivotal for organizations to build trust with their users and deliver solutions at scale.

The race to market often involves swift, short-term decision-making so that minimum viable products are delivered on-time and within budget. While these decisions may lead to a successful product launch and immediate revenue, they also create vulnerabilities and organizational exposure. This can result in cyberattacks, mishandling of consumer data, regulatory scrutiny, reputational damage, and operational disruptions, each eroding consumer trust. Organizations are then forced to reevaluate the architecture of products, the composition of processes and controls, and the cross-functional implications of reactively mitigating risks or complying with regulations. The resulting solutions may be disruptive, temporary, or require a costly investment to reengineer from the ground up.

Embedding and executing Compliance Engineering during the initial stages of planning and product development reduces the need to allocate costly resources for retroactive design corrections. A strong foundation of compliance-engineered products equips organizations to protect and scale digital trust, comply with regulations, and foster innovation. Compliance Engineering is not just a business imperative but a critical response to evolving customer expectations, expanding regulatory obligations, increasing competition, and rising cost pressures. By embedding Compliance Engineering from the onset, organizations can build trusted products that proactively reduce potential risks, reduce external pressures, and achieve sustainable growth and long-term success.

Though no two organizations are the same, solutions are readily available to improve the efficiency of development while expanding compliance coverage. Considering the size, complexity, maturity, and goals of an organization, it's important to understand which Compliance Engineering solutions and practices have demonstrated effectiveness in reducing costs and building trust without compromising product innovation.

How Deloitte Can Help

In today's highly competitive, rapidly evolving, and regulatory-driven technology landscape, organizations need a trusted service provider who understands the complexities and importance of achieving compliance maturity. Deloitte's global team of specialists brings together extensive industry experience and cutting-edge Compliance Engineering solutions to equip our clients with the tools and capabilities to efficiently garner trust with customers, achieve compliance, and remain competitive.

Our tailored approach to building trusted products is centered on providing risk-aligned and tech-enabled Compliance Engineering, including but not limited to:

Proactive Compliance: Deloitte helps organizations anticipate regulatory changes and implement proactive measures that focus on continuous compliance. This reduces the risk of non-compliance and enhances operational efficiency.

Trust by Design: Deloitte emphasizes the importance of building trust into the design and development process. This includes incorporating privacy, security, and transparency features from the outset, assessing and designing products and services that are not only compliant, but also trusted by users.

Integrated Technical Solutions: Deloitte provides integrated compliance solutions that leverage the latest technologies, such as automation, AI, and privacy-enhancing technologies (PETs). These solutions streamline compliance processes, reduce manual effort, and provide real-time insights.

Deloitte's global **DIGITAL TRUST & COMPLIANCE ENGINEERING** team comprises of compliance, safety, AI, engineering, regulatory, economics, data privacy, and forensic specialists who can help organizations formulate and implement their response with end-to-end, multi-disciplinary support for each stage of the digital product and platform development lifecycle.

Cases Studies

Intelligent Reporting & Dashboard

The client faced challenges in processing disparate data insights from various functional silos to inform business strategies from a privacy and security perspective. To address this, Deloitte assessed the organization's data landscape to identify high-quality signals related to organizational performance, privacy risks, and the integration of people and technology. Deloitte then developed a strategy to enhance the company's intelligence capabilities, from evaluating data and deriving insights to creating appropriate forums and reports to support leadership decision-making. To improve executive reporting, Deloitte designed a business intelligence dashboard that unified key data points for near real-time analysis. These efforts helped the organization streamline its disparate data and unlock insights that elevated its organizational objectives in a volatile regulatory landscape.

Privacy, Safety, and Security Automation – Policy as Code

The client faced challenges overseeing and maintaining guardrails for internal usage of its Cloud products. Deloitte served as a trusted advisor to the organization to develop a generative AI application to extract key information from the company's internal service tickets and performed detailed analytics on the outputs, identifying frequently requested products and historical trends to implement targeted security and privacy guardrails. Beyond advising on guardrails, Deloitte provided guidance on potential growth areas, including automating response generation for future requests, implementing conditional rules, and developing accelerator codes and configurations. These efforts helped the organization to pinpoint focus products for improved governance, establish guardrails to enhance compliance posture, and identify automation opportunities in compliance.

Automated Field Mapping for Cloud Data – Data Governance

The client wanted to confirm the efficacy of controls in place for customer data collected via their cloud application programming interfaces (APIs) and faced challenges in mapping 6,000+ distinct API fields to their backend control systems. The main issue was inconsistent naming conventions between the fields and backend systems, historically requiring a time-consuming manual effort prone to errors. Deloitte served as an advisor to the company in leveraging GenAI prompt engineering to perform "fuzzy mapping," utilizing few-shot prompting techniques to reduce LLM "hallucinations" and promote logical step-by-step processes. These efforts resulted in the mapping of ~85% of the fields in less than two hours and provided a mechanism for the organization to reproduce mappings automatically going forward, saving time and costs while also improving their ability to respond to regulatory requests.

Contact Us

Please reach out to our team if you would like to discuss these topics in more detail.

Tanneasha Gordon
Principal
Data & Digital Trust Lead
Deloitte & Touche LLP
tagordon@deloitte.com

Arpan Tiwari
Managing Director
Edge AI and Alliances Lead
Deloitte Consulting LLP
arptiwari@deloitte.com

Esther Choi Ohm
Senior Manager
Data & Digital Trust
Deloitte & Touche LLP
eschoi@deloitte.com

Luke Jacobson
Manager
Data & Digital Trust
Deloitte & Touche LLP
lujacobson@deloitte.com

Josh Lee
Manager
Data & Digital Trust
Deloitte & Touche LLP
joshslee@deloitte.com

Jacky Nguyen
Manager
AI & Engineering – Industry Solutions
Deloitte Consulting LLP
jacnguyen@deloitte.com

Pauline Pang
Manager
Data & Digital Trust
Deloitte & Touche LLP
paupang@deloitte.com

Deloitte.