Deep Science Publishing
https://doi.org/10.70593/978-93-7185-253-1_6

DeepScience
Open Access Books

Chapter 6: Building compliance-focused infrastructure with robust data security and operational transparency

6.1. Introduction

Cloud platforms have rapidly evolved to support critical services. Many State and Local Agencies are increasingly using commercial cloud services to fulfill policy missions due to their speed, efficiency, and accessibility; especially, during the pandemic times when traffic surges and remote workforce demands are met utilizing those cloud services. The cloud-enabled applications and services are developed and deployed rapidly. However, the availability of these services is also often impacted by outages. These outages happen due to Denial of Service attacks that compromise the shared security posture of cloud-enabled services, vulnerability, and misconfiguration exploitable through cascading and amplitude overspill effects, hyper-scaling resource and burst behavior that overshoot for resources, functional integrity risks, and physical data center threats. As sensitive data moves into cloud services, so does concern for data security. Therefore, it is crucial to build infrastructure that defends against such outages. Such additional defensive measures can help agencies manage their workload demands without interruption, fulfilling their mission (Ekundayo & Ikumapayi, 2022; Adio et al., 2025; Al Khateeb, 2025).

The idea of hardened infrastructures is not new, nor is the concept of Defense-in-depth. Hardened infrastructures have been developed and deployed to meet mission-critical needs through various mixes of technologies in regulations. Infrastructure such as ITAR and Controlled Unclassified Information push the need for Government Cloud. But, for non-edu state agencies, perhaps the mission utility of Commercial Cloud Services outweighs the risks. For those services, it is the essential advisory role of a Cloud Service Provider and an Internet Service Provider to protect the services considering the risks hence suggesting security as well as compliance guidance. This security guidance not only places an obligation on the Cloud Service Provider and Internet Service Provider to audit their cloud services but also a level of instruction for the SLO of an agency on business services for their secure operations in the cloud service ecosystem (Kalinin & Gonchar, 2024; Owoade et al., 2024).

6.1.1. Background and Significance

Blockchain emerged in late 2008 as a decentralized digital ledger created to facilitate peer-to-peer electronic cash transactions and has quickly gained attention across both public and private sector applications. Given its unique properties of decentralized trust, transparency, auditability, immutable data provenance, and resistance to data alteration or corruption, blockchain is being considered in multiple aspects of both authoritative identity and digital credentialing. Blockchain can enable decentralized infrastructures for the authority to issue, verify, validate, and pressure-accept trusted digital identities, and for trusted digital identity credentialing. This is of paramount importance to functioning democracies globally for several reasons: A large number of private and public agencies issue identity documents, commercialized or otherwise, and coordinate amongst themselves to provision access to rights, benefits, and services; Individuals often hold several identities issued by different agencies, and rely on different entities to cross-verify between them; Identity documents may influence lives dramatically by determining the entities within which resources are allocated, protected, and privileged.

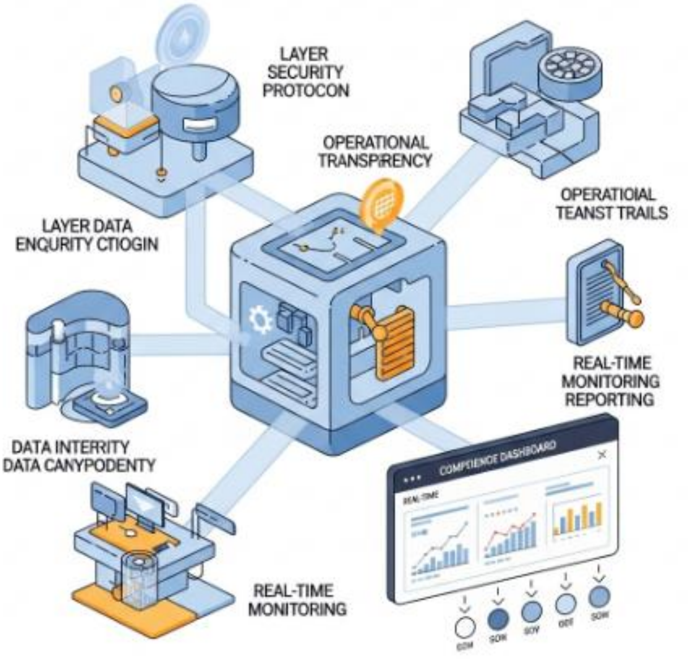

Fig 6.1 Building Compliance-Focused Infrastructure with Robust Data Security and Operational Transparency.

The recent rise of mass populism has amplified calls for greater accountability in government agencies. Clear tracking of the provenance of identities being issued, and the validation of claims made against them is vital for strengthening both physical and cybersecurity for individuals, the collective benefits that must be administered without malfeasance from agencies trusted with provision and upkeep, and the rights and privileges that these identities convey on holdouts. Any acceptable and trusted decentralized blockchain-based digital identity infrastructure must have some mechanism for backing the identity constructor services – the public or private agencies, or a combination of the two – to assume accountability, transparency, and liability. Blockchainsand their often-ubiquitous smart contract programming environments can provide a mechanism to automate a large part of this accountability.

6.2. Understanding Compliance Frameworks

In today's regulatory landscape, every business finds itself working with and complying with an assortment of technology and industry partners. Each partner has its own set of compliance standards that your organization needs to assess and manage over time. More often than not, maintaining compliance over time can be a key gating factor in business expansion activities, stymieing business growth if it is not maintained throughout the business cycle. Accordingly, businesses should consider compliance/security requirements as an ongoing activity, one that addresses existing requirements and builds up to fulfilll additional security controls. For technology and service partners in particular, the responsibility of being compliant not only drives the business foundationbut is also fundamental to gaining traction and trust within the marketplace. Established reputational perspectives such as providing a compliant service are generally an expectation today. This is where Operational Transparency is an important pillar in establishing trust in your service providers. Why not join the ranks of other organizations and utilize Operational Transparency to demonstrate, continuously, that your organization is a trustworthy partner? It provides a low-cost, consistent communication mechanism to the marketplace, and demonstrates to your diligent customers and partners, through a system of regular notifications, that you are a business of integrity.

In the following chapters, we will first provide a primer on compliance concepts: compliance vs certification; regulatory bodies, and compliance structures, review common compliance standards and speak about control sets associated with them, provide examples of how various services or product categories conform against specific compliance standards, and go through some advice on how to use compliance frameworks to your advantage. Then we will discuss Operational Transparency and its pillars of Transparency, Completeness, Assurance, and Trust; Situational Flair, Auditing Comments, Soft Compliance, and Translated Business Vision; Micro-Compliance; and methods for establishing Operational Transparency. Finally, we will wrap up by discussing Transition Management / Micro-Compliance, and roadmaps for Operational Transparency. So let us dive in!

6.2.1. Overview of Compliance Standards

Many businesses today depend on obtaining and preserving information that both meets customer needs and fosters trust. This often-difficult task has been made easier through the establishment of many compliance adherence frameworks. Compliance infrastructure is a consumer’s protection against dangers from an organization that fails to adhere to best practices defined by regulatory bodies. This section defines, in increasing levels of detail, the types of compliance frameworks and the organizations that promulgate or adhere to the various standards. At a high level, there are two types of compliance standards: Global and Regional. Here the focus is on region-specific frameworks since the compliance definition space is large and rapidly changing. Any compliance standard must have a governing entity, such as a committee, whose function is regulation and the responsibility of enforcing punishment if the regulations are not enforced. The committee also deals with consumer grievances and issues and attempts to address them by recommending or changing implementing guidelines. Compliance can be enforced through audits on a given time cycle for the organization being audited. Depending on the severity of any offense discovered, an organization may receive either positive or negative enforcement. Positive enforcement indicates that certain penalties are being levied for a specific time for minor violations, whereas negative enforcement indicates suspension or revocation of all or part of the operations for gross negligence or violations of a severe nature.

6.2.2. Regulatory Bodies and Their Roles

Data security and privacy laws are created and enforced by specialized government agencies around the world. These agencies create and enforce regulations designed to protect specific types of data and apply them to specific organizations or sectors. To get a comprehensive understanding of their obligations, organizations must understand which laws and regulations apply to them and their customers, and who is responsible for each law.

Many organizations leverage the multiple compliance standards from third-party, nonprofit organizations. Such organizations do not have the legal authority to fine non-compliant organizations; however, the standards they create are often based on laws and compliance frameworks set forth by government agencies. The organization’s compliance with these third-party standards may be important to customers and may need to be demonstrated to do business with specific customers or sectors.

Other organizations and sectors must comply with federal and state privacy laws created and enforced by specific regulatory bodies. Within the government, agencies are designated to govern specific types of information. For example, one agency governs personal data privacy enforcement for consumer data and another governs data privacy for telecommunications companies. Other industry sectors have laws enforced by regulatory bodies that have the authority to issue fines or penalties in the event of a violation of the law. For example, hospitals are governed by specific regulations and a department has the legal authority to administer and enforce compliance within the healthcare sector. Another act governs the financial sector, and a bureau has the legal authority to issue penalties for violations.

6.3. Infrastructure Design Principles

Whereas the preceding subsection raised the question of why manage security and compliance from infrastructure, this subsection builds upon the notion of compliance-focused infrastructure and presents several design principles for creating it. Focus strictly on foundation principles of scalability and flexibility, and decide on operational policies and their automation later. Cloud-provided resources have elasticity in their native properties; words like elastic burst and elastic scale were first associated with hardware-provisioning services. In that, the definition of infrastructure is limited to providing only the mechanisms of support for upper layers. However, it is mechanisms that will be the first items needing to mature—cloud-provided resources are inherently volatile, and depending on them without thought can lead to problems later. This is why, for the near future, workloads are likely to require an underlying base that is either specialized, and thus very flexible and scalable but also tightly controlled; or one that is, so to speak, generalized—cloud-provided, and thus not tightly controlled—yet thoroughly prepared for compliance, and thus containing the necessary glue that makes it flexible and scalable. The validity of this decision will ultimately emerge when time permits no longer strict operational requirements. The need to provide compliance is essential, but is not near in most cases; what should be allowed is defining a staged approach; infrastructure, conforming to the regulatory considerations, resource policies, and configuration states necessary to provide audit, must be defined at first, along with the necessary procedures for quality assurance and management; adding the day-to-day log collection and event management processes can then be added as an addendum.

6.3.1. Scalability and Flexibility

Modern cloud infrastructure supports as many workloads as necessary to serve the business workload. Large businesses face 1000s of workloads that require infrastructural capabilities. Businesses will have different environments for development, testing, staging, and production. Similarly, multiple production environments for different functionality might be present. Infrastructure management systems and databases for the enterprise would have to be configured with these environments listed. This should be a one-time execution that once completed configures the environment for 1000s of workloads under different business units and environments. Thereafter, as a business unit or an application grows or a business strategy for an application changes, resources are added, modified, or deleted from this environment. The same functionality would be available at the database level as well. The cyber security team would also need to configure rules before the e-workload starts for the day or week at the load balancing, firewall, and server levels. Configuring auditing and logging access roles may also vary over time and may be formalized in such a manner.

As business strategy changes, the compliance requirement too may change. In the traditional IT world, all firewall configurations and rules were set and the requirements defined. In the cloud era, accessibility and business change, audit and compliance checks have to be able to check firewalls and rules, and reports have to be generated to check for any violation. In the above scenario, multiple reports are required for a business from various systems to check compliance with regulatory laws. Most cloud vendors provide such solutions as part of their suite, but the availability of such reports at the level is scarce, which is the first stage of configuration before the workload starts.

6.3.2. Integration of Compliance Features

When designing our cloud infrastructure, we integrated compliance features and data protections at multiple levels. This is a proactive approach to compliance design. We worked on and continue to work on meeting the compliance regimes relevant to our clients, but we didn’t wait for audits to take place for our systems and features to help clients mitigate their risks related to the cloud, compliance, and mitigation subject areas. Our design approach was and is to store client data in a cloud configuration where regulatory requirements, such as data residency or data classification, were or are taken into account and implemented. Some of our services feature alternate configurations, such as different supported security standards, encryption methods, or geographic locations, in order to support different client requirements.

Integration of compliance features means everything from network architecture, which includes firewalls, DMZs, and intrusion detection/prevention systems, as well as background data processing and reporting, to front-end web and mobile applications having sensitive input validation and offering transparent data usage practices and consent collection. This latter front-end usability aspect may seem more UX-focused than compliance-focused, but as clients interact with our services, we want to build trust by enabling data usage control and visibility through the client user interface. It's not enough to merely present a big privacy policy in the footer of the web page and expect clients to click acknowledge consent because it mentions cookies and analytics services. Instead, controls related to data protection, along with a clear discussion of why data will be collected, should be transparent and, as possible, customizable by our clients.

The implementation of our services is designed the same way, integrating compliance features such as definable data residency through supporting multiple cloud regions; logs of admin activity and data access by product and clients themselves; records retention and expiration controls; and product configuration for data classification, use, and sharing.

6.4. Data Security Strategies

Data security is an increasingly critical concern for organizations and their clients, especially in the context of tight deadlines and the placement of refugees. Stakeholders

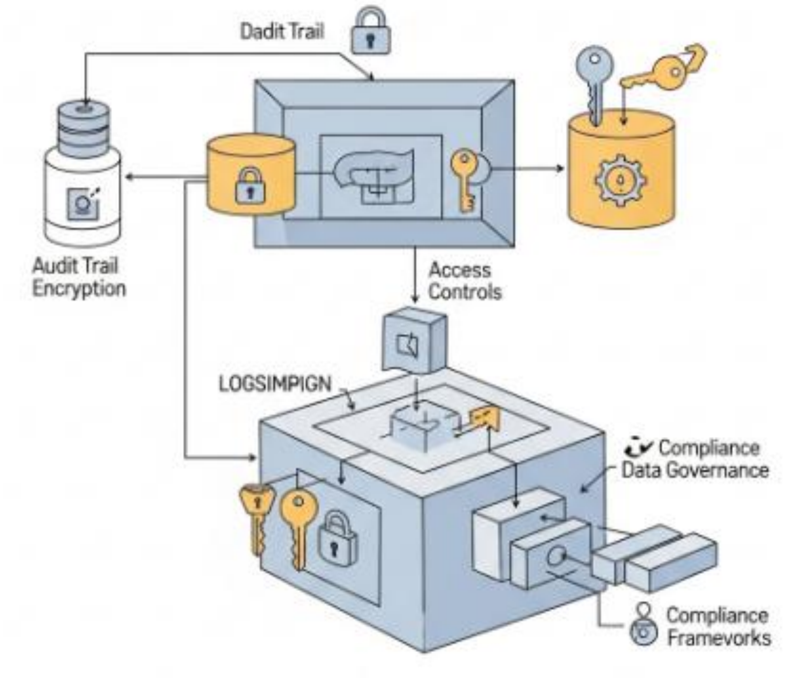

Fig 6.2: Data Security Strategies.

at every level are understandably anxious about the security of their sensitive protected data, from a patient's health information in electronic form to their records on a printout or CD. Furthermore, clients expect high levels of performance and accountability from the organizations they partner with. Achieving this credibility and reliability requires organizations to have smooth and effective plans and systems in place. Security breaches, theft, and non-compliance with regulations will undermine any claims of competence and reliability.

The breach of sensitive protected data can cause severe and lasting consequences, not just for the affected organization, be it the immediate client or a partner in the data pipeline, but also for the owner of the data whose confidentiality has been breached. Organizations should have a set of well-defined policies and security mechanisms in place through which they manage and regulate data access. By employing these data security strategies and techniques and maintaining operational transparency, organizations can establish and maintain the trust necessary for responsible and credible partnerships. This section discusses data protection mechanisms at a high level. These data security techniques are complementary, and organizations can choose to implement any combination of them for their data repository. This section discusses three major strategies: encryption, access control, and incident response planning. We provide additional descriptions of these strategies below.

6.4.1. Encryption Techniques

Although unencrypted data is the easiest form of data to work with, it is also the least secure and, as a result, the most valuable to attackers. Organizations earn compliance and trust by minimizing risk to individuals and the organization by deploying risk strategies that include encrypting sensitive data where possible and, importantly, encrypting it throughout its entire lifecycle. Encryption techniques can broadly be placed into two categories: authenticating and non-authenticating.

Non-authenticating encryption techniques, such as block ciphers and stream ciphers, are the bulk of encryption techniques in use today. Data that is encrypted with these techniques is often accompanied by a message authentication code (MAC) that ensures the data has not been modified while encrypted. With these types of approaches, however, there is a gap in data lifecycle protection because when the MAC is produced, it is not encrypted. For many data protection solutions, such as those used for file-level encryption, database encryption, and cloud storage encryption, non-authenticating encryption keys are stored somewhere in their cleartext form, representing another weakness in complete lifecycle protection, although some solutions also utilize a MAC. In general, the security of MACs is equivalent to the ciphers used to implement them, making them susceptible to deep cryptanalysis. Encrypted data with possible cleartext

MACs is also easy for attackers to inadvertently modify. The most common method of performing MAC on data is the widely used hash function approach. Because hash functions are only secure against random pre-image attacks, this is a concern. Other techniques to address this vulnerability exist; some examples include combinations of stream and block ciphers.

6.4.2. Access Control Mechanisms

The minimum security protection mechanism for any Office 365 tenant is password authentication. It is possible to increase the level of protection of accounts in Office 365 using conditional access, multi-factor authentication, or more dangerous alternatives such as self-service password reset and password-less authentication, but let us now focus our attention on password authentication mechanisms. If we get a list of usernames from any source, it is possible to check if any of the usernames have an account in the target tenant organization with an account enumeration attack. If many users have valid accounts we can use a valid account or brute-force attacks against one or more of the companies to acquire a user password and become an authenticated user of the tenant organization.

If we succeed in acquiring a valid account, by default, we will not be able to do anything because all user accounts require additional privileges to perform any useful operation on that account. These additional privileges are generally assigned to one or more Security Groups. Office 365 assigns users to at least one security group that has no privileges associated and users might be aimed for specific service permissions, and all resources are protected against unauthorized access by specific permission assignments to those Security Groups. On the contrary, the Office 365 built-in roles have minimum privileged permissions assigned to users who have to perform administrative operations, allowing them to take full control of tenants just by using the assigned roles.

6.4.3. Incident Response Planning

Cyber threats are ever-present and successful preventative measures cannot be expected 100% of the time. Hence, organizations are expected to have adequate security policies and procedures in place to address post-incident crisis management. An Incident Response Plan (IRP) establishes a strategy identifying the processes the organization will follow in response to a variety of security incidents. An allocated response team should formally test the plan at regular intervals so that they would have practiced and honed their skills for responding to real incidents. The team should include members from relevant security functions such as IT, legal, public relations, human resources, compliance, forensics, and senior executives. Detailed response strategies should be included, addressing issues such as: whether outside agencies such as law enforcement officers will be contacted. What incident investigation and incident validation measures will be employed? What forensic tools, independent third-party forensics experts, and services will be utilized? How backups will be used? What methods will be used to preserve evidence? How will systems and applications be patched? Documentation of the incident should be comprehensive.

Regulatory guidelines and industry standards require that any breach of private data such as personally identifiable information, financial data, or medical records be notified to the affected customers within prescribed timelines. Also, the incident needs to be investigated, and then appropriate remediation actions must be reported back to the appropriate regulatory and oversight authorities documenting lessons learned and the steps essential to avoid similar breaches in the future. Failure to enact these incident response requirements can lead to significant penalties which may even cripple the organization.

6.5. Operational Transparency

The importance of user trust cannot be underestimated. It has been shown that users are much more likely to share sensitive data when they are clearly and effectively informed about what will happen to their data, and for reasons why they should trust the service to do the right thing. While companies can and will gain user trust through various forms of marketing, it has also been shown that verifying the service's responsible data handling practices is the most effective way to gain considerate user trust. Furthermore, regulatory bodies are leaning toward policies with an emphasis on transparency, with requirements for privacy and data security notices, labeling, and auditing. That being said, it is difficult to construct a transparency strategy that is "just right" for a typical user. How many privacy notices have you seen when signing up for an account? Providing too much transparency can induce information overload; protecting users from excessive complexity by omitting subtle details and jargon can, at the other extreme, seem patronizing and overly sardonic. Operational transparency can ameliorate this issue, in conjunction with other personalization elements.

One form of increasing operational transparency is helpful guides that walk a user through the functionality of the service, such as a data access or deletion procedure. But while these can help users traverse a process they may find confusing, or at least they may find one particular interface confusing, the more natural extension of providing operational transparency is to deploy user action monitoring and reporting tools, accessible in a manner likely to be useful yet unobtrusive, that allow the user to simply "look and see" what is going on. In this area, or junction with permission for data sharing, there is also a clear trend towards dynamic audit tracking of how users' data is being used, extending audit logs for individual services or functions to cover all actions on those data, across functions.

6.5.1. Monitoring and Reporting Tools

Monitoring and reporting tools are critical for establishing transparency of information and decision-flow linking policy, use, and reported outcomes of data use. Infrastructure investment and operations should be monitored in a manner that is clear to infrastructure providers, data users, and the affected populations across the data life cycle, at the individual, group, or population level. When adverse outcomes of data used for any of the groups are reported, the infrastructure provider should be responsible for explanation, justification, and rectification. Such talks with the impacted communities or groups, to the extent possible, amplify the voice of communities.

The tools used for monitoring and reporting should be appropriate for distinct phases of the data life cycle and the different stakeholders. These tools should operate at a variety of levels, including individual data items, aggregate usage, and data handled by specific entities, users, or types of users. These tools need to provide information reported in a standardized format and in real-time to facilitate review and explanatory conversations among all participants, including representatives from the communities or groups who are impacted by the outcomes. Such conversations would also help create public trust, cooperation, and advocacy for correcting adverse impacts and help in preventing future harm Furthermore, other tools could address specific phases. For example, forensic auditing tools have been developed for the collection of datasets and secure multi-party computation that permitss software verification that distinct entities adhered to prescribed protocols.

6.5.2. Audit Trails and Compliance Checks

Audit trails and compliance checks are not so easy to add on. Often they require significant antecedents, especially at the outset of the project's data journey, and implementing them later is extremely expensive. Having a clear data audit trail and a plan for compliance checks adds quite a bit of cost to a pilot but pays off massively in terms of reducing future costs in full production.

Here are some aspects to keep in mind to help ensure that you are set up for eventual success.

You may or may not be doing everything in version-controlled infrastructure code. If you are building infrastructure using modules or plugins that visually set up cloud resources in a blueprint manner, or pointing to higher-level managed services, it may be more difficult to pull even more layers of transparency throughout your services. But it may be easier given fewer lines of code to manage. At least you should be plugging in version-control information and an audit layer to the services you have little field-implemented custom code.

Your prototype services might be point-to-point and monolithic. In which case you should at least consider how you might segment them into separate components for actual production so that specialized checks for various aspects of these services could be added. Even if you don’t make them separate microservices at the beginning, having a plan that is well-documented should make it easier to peel off parts later, if needed. It is certainly much easier to add checks to services that take inputs and produce outputs with defined data formats, as opposed to services that just change an internal state.

6.6. Risk Management Framework.

Risk management should go beyond responding to incidents. It should be aimed at both avoiding known and expected incidents as well as reducing the potential impact of risk events that cannot be avoided. Developing an effective risk management framework requires an articulated enterprise risk management strategy that outlines the firm’s philosophy towards risk, establishes risk governance processes and structures, clarifies roles and responsibilities related to risk issues, and specifies key directional risk policies and limits in critical business areas. With definitions and supportive structures in place, risk areas can be more effectively identified, assessed, reported, and discussed. Risk management strategy is at its most effective when it is clearly articulated, embedded in the firm’s culture, consistently practiced, and integrated into the firm’s business operations.

Risk strategies should be driven by risk tolerance as determined by senior management and the board of directors. It is an integral part of the company’s strategic planning and capital allocation processes supported by ongoing communications from the board and senior management about the significant role that risk plays in the conduct of the company’s business. All operational units should understand the importance of managing risk in their particular areas of responsibility and how their activities contribute to the company’s overall risk profile. Knowledge of risk tolerance should help inform company operational units as they make near- and long-term decisions and is typically incorporated into macro-level and business-unit forecasting and planning processes. Planning cycles vary by company, but business-unit governance processes and operational metrics should align with decisions being made in the strategic planning process.

6.6.1. Identifying Potential Risks

Identifying and managing risks associated with data protection and security issues in any organization's infrastructure is usually a simple if not straightforward task. Established, regulatory-driven rules and guidelines give a lot of information on what areas we need to review in order to configure our infrastructure properly to protect it against all malicious data-handling actions that endanger our organization's business continuity. Questions we need to answer and review may include for example:

- Are there data exfiltration risks associated with running an API that allows outsiders to query sensitive data directly from our databases?

- Have we configured appropriate measures to avoid exposing sensitive data through log files, including assigning proper access rights for log files, configuring log purge jobs, encrypting log files, and the like?

- Can a non-privileged insider run a script that exhausts the resources of a multi-tenant architecture where many other companies are running their operations in a separate business context?

- Does our multi-tenant architecture intercept and use sensitive data from multiple organizations before pushing it to a commercial third-party vendor?

- Do we have the means to quantify risk levels associated with the answers to the previous questions?

- To what extent can we trust all third-party service vendors that are part of our infrastructure deployment?

- Are we forced to accept the use of sub-vendors by any third-party service vendor who collects, processes, or stores sensitive data on behalf of our organization?

6.6.2. Mitigation Strategies

Mitigating privacy risks in digital containers can be enabled by several substantive and technical measures including: Firstly, including transparency, purpose limitation, and data minimization measures, to prevent inappropriate processing, which iscritiis criticallablishing a foundation for containerized DTC services. Transparency helps address and service the risk of non-consultative or undue uses of personal data that occurs with the commercial use of ubiquitous and pervasively applied data augmentation, profiling, and targeting. This is because privacy harms primarily arise from activities such as tracking, monitoring, exposing, trading, or automating adversely impactful decisions, rather than the collection and storage of data per se. This indicates that all levels of data processing require express permission from the data subject, and that data must be adequately and securely disposed of once no longer needed. Purposes should accompany the service and be understandable, proper, and designated, justify the necessary processing operations, and be established in express consent, and premium consumer services could offer clearer fit-for-purpose containers. Respecting limitations that require that such purposes should not be excessive, hidden, undetermined, vague, excessively broad, violate future expectations, or unreasonable prevent harm from bottling up data for use in questionable ways and help establish a baseline of compliance.

Secondly, data classification, restricted access, enhanced security through encryption, anonymization, data availability, and audit trails protect against excessive, insecure, and improper use of unnecessary data. Classification allows companies to identify what data consumers are allowing them to use (and for what purposes), and what data is being held but not used under the principle of data minimization. This can inform the decision to delete the latter, as well as the application's decision on what user data it can access and how it might do so, as well as what security measures should be taken against insider threats. Third-party service providers require controls, such as preventions against excessive access to, or transfer of, user data through privileged accounts, or explicit user consent, to ensure the data they process is not stored unnecessarily.

6.7. Conclusion

Contract and regulatory compliance are constructs assembled from multiple standards and requirements. Many are fungible and are not crypto-specific, for example, tax regulations. Some – such as anti-money laundering laws – have anchors in traditional business and are seldom clear in their interpretations. Others are designed to harvest the supposed uniqueness of crypto and require special familiarity. The challenge for compliance-motivated crypto organizations is to check all compliance boxes unique to their properties. Only by matching these boxes to specific authorities and their institutional requirements can crypto get on the path to compliance. Self-education and community sharing of knowledge and tools have been emphasized as important in this process. Crypto organizations and users will need to formalize this community knowledge into bona fide accessible public resources.

The compliance infrastructure of crypto has been largely opportunistic. Some crypto products, such as exchanges, are doing compliance the right way early. Others, such as DeFi and cross-border payments and token transfers, are going about their businesses with scant regard for compliance. Stricter requirements being introduced both by governments around the globe, as well as entities in the crypto ecosystem itself, are expected to spur innovation, including the application of avant-garde technology. Deficiencies of the infrastructure will be addressed. More crypto organizations will be set up for the express purpose of service compliance in-house or in conjunction with the compliance services of traditional finance. In-house compliance will be informed by cross-industry experience garnered through crypto's passage into the mainstream.

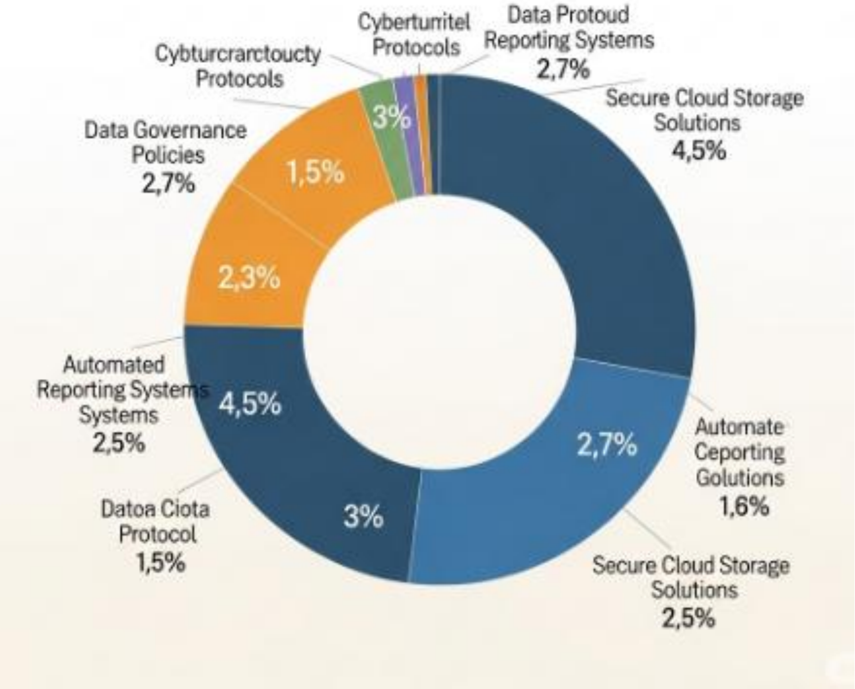

Fig: Building Compliance-Focused Infrastructure with Robust Data Security and Operational Transparency.

6.7.1. Future Trends

Building compliance-focused infrastructure to support enterprise blockchain applications is definitely a complex, multi-faceted problem, especially considering the lack of comprehensive regulations developed specifically for the governance of blockchain ecosystems and infrastructure. However, over the next few years, a large number of industry stakeholders, from regulators and governmental organizations, to crypto-native and enterprise blockchain companies, and business use case-focused tooling developers will contribute to a joint effort at creating this infrastructure. Doing so presents an enormous technical implementation challenge, yet we believe creates the potential to develop an equally enormous market opportunity. Within the next few years, we expect to see the availability of a range of tools and services to help governance bodies and other stakeholders such as treasury and oversight committees or compliance administrators to introduce compliance, security, and risk management technologies and practices that will enable the seamless embedding of compliance and transparency constraints as key components of their blockchain activity. This will include, for example: Automated function and code scanning to detect and identify potential risks and compliance failures. Support for customizable and modular on-chain compliance and audit logic. Support for non-relational and distributed transaction data regulatory compliance frameworks for on-chain activity. Seamless off-chain, on-chain, and cross-chain analytics of transactions to confirm intent and audit compliance. Support for contractual TDs, risk-weighted payments, and layered on-chain economic coordination designs. Enterprise infrastructure providers will move quickly - building partnerships with policy, governmental, legal, and regulatory experts to connect their compliance technologies with the industry-specific compliance requirements of both the enterprise blockchain applications of their clients/users and the regulators responsible for monitoring and auditing their activity - to provide enterprises with compliance-oriented post-transaction audit infrastructure and transaction monitoring during blockchain activity.

References

Owoade, S. J., Uzoka, A., Akerele, J. I., & Ojukwu, P. U. (2024). Cloud-based compliance and data security solutions in financial applications using CI/CD pipelines. World Journal of Engineering and Technology Research, 8(2), 152-169.

Kalinin, O., & Gonchar, V. (2024). Strategic Partnership as a Factor in Sustainable Development and Compliance Adherence.

Adio, S. A., Ajirotutu, R. O., Olayiwola, R. K., Erinjogunola, F. L., & Sikhakhane-Nwokediegwu, Z. (2025). From Compliance to Competitive Advantage: The Strategic Role of HSE in Business Sustainability.

Ekundayo, F., & Ikumapayi, O. J. (2022). Leadership practices in overseeing data engineers developing compliant, highperformance REST APIs in regulated financial technology environments. Int J Comput Appl Technol Res, 11(12), 566-577.

Al Khateeb, H. (2025). Increasing Data Protection Compliance for Remote Workers (Doctoral dissertation, Northeastern University).