

Unlock Tomorrow: Mastering Regulatory Compliance





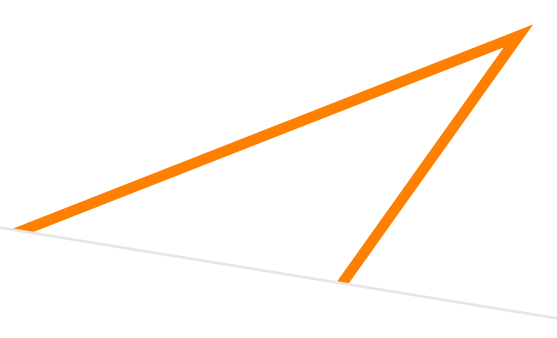
The cornerstone of trust is compliance

Trust forms the bond between an insurance company and a policy holder. If a policy holder cannot rely on an insurance provider, broker or point of service, the bond will be severed and the policy holder will look for a more trusted provider or service.

Insurance companies have zero room for error in the eyes of their policy holders, and must fulfil all agreed obligations and pay out claims fairly and consistency - no ifs, ands, or buts.

And to build trust requires insurance companies to adhere to strict compliance regulations. Regulations which offer protection for policy holders and promote a sustainable, long-term insurance industry that defines success and reputation through sound risk management practices and market integrity.

But regulatory bodies within the insurance industry today are more stringent than ever in enforcing compliance and imposing penalties for violations in the forms of fines, legal actions and sanctions. So, it stands to reason that compliance efforts must be treated as vital to success and **business continuity**, and rightly assigned the highest priority within insurance companies.



This whitepaper will discuss the key challenges faced when dealing with adherence to compliance, and how Keylane partners with insurers to support their full regulatory compliance and safeguard their ongoing success as leading providers within the insurance industry.

Topics that will be covered are:

- ▶ Understanding the critical role of the compliance officer and its relation to business continuity.
- ▶ Investing in, maintaining and testing resilience and fail-over systems.
- ▶ Making sense of incident reporting and effective risk management.
- ▶ Complying with data protection & privacy and the evolving demands of outsource oversight.

Regulatory bodies within the insurance industry today are more stringent than ever in enforcing compliance and imposing penalties for violations.

The role of compliance officers

The role of a compliance officer within the insurance industry has evolved measurably over the years, and is now a high stakes, critical function that directly influences and supports ongoing business continuity.

Where once the role of compliance officer meant the need to administer and maintain instructions and guidelines, the role has been vastly elevated to ensuring strict adherence to legally anchored compliancy and regulation laws. As such, compliance officers are now **key advisors** to an insurance company's board of directors, working diligently to support responsible business operations that act in full accordance with applicable laws and regulations.

Compliance officers must also manage **complex issues**, such as overlapping regulations and country specific vs regional requirements. Their wider responsibilities encompass monitoring changes in laws, industry standards and advise management, as well as developing compliance policies, procedures and systems, and collaborating with other departments to **ensure regulatory requirements** are met across the business.

The complexity of compliancy and regulation management means that several common strategic topics and pain points tend to arise. However, with nearly three decades of experience, Keylane is uniquely positioned to ensure full compliancy and peace of mind for all modern insurance providers.

Strengthening resilience

Regulations, such as EU/DORA and BAFin/VAIT, seek to enhance the **resilience** of both financial market participants and infrastructure providers against IT failures and cyber threats. In practical terms, this

means insurers are required to implement a number of processes and systems to mitigate operational risks. This includes implementing fail-over systems and data back-up solutions, and just as importantly, making sure these systems are **properly tested**. When all is said and done, the purpose of a disaster recovery plan is not only to guarantee business continuity in the event of a serious system malfunction, but to also grant stakeholders full peace of mind in an insurer's business operations.

Additionally, many insurers have stepped up their investments to protect against cyber-attacks. But to keep ahead of these threats, investments in cyber security demand ongoing, long term commitment, and threats and vulnerabilities must be constantly monitored, while preemptive action must be taken when necessary.

Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) is a EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025. It aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption. DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.

Fortifying redundancy and back-up systems

In the event of critical system failures, insurers are required to have redundant systems on standby to ensure that critical business processes and data are always available and fully functional. Such a fail-over environment, with its own independent hardware, network connections, power supplies and data storage, must be instantly ready to provide full business continuity.

And these requirements apply to the entire application landscape, not just new core systems. The application landscape must be clustered and segmented, requiring firewalls be built and access rights and privileges redesigned. This is not a simple task, and can be especially challenging for insurers running core operations on legacy systems and platforms, as older software architectures are limited in ability, while duplicate standby mainframes are expensive to maintain.

With these challenges in mind, today's insurance providers are looking to invest in core platforms that can be fully hosted and run in a cloud environment - by outsourcing the demands of ensuring full compliancy to a partner, providers are also guaranteed full back-up and fail-over functionality.

Addressing these needs, Keylane hosts its Axon platform independently for every client within a fully clustered, geographically separated and high availability environment. Additionally, each client is fully supported by a dedicated team of Keylane experts.

Disaster recovery planning and testing

Updated regulations mean that insurers must now have comprehensive disaster recovery plans. These plans must demonstrate that the system redundancy in place is adequate, functional and fit-for-purpose. A comprehensive disaster recovery plan should outline **all necessary recovery steps** to be taken in the event of IT system failures or data disruption events.

Put more bluntly, governing bodies force insurers to **test** their disaster recovery plans to guarantee their effectiveness or to expose flaws. It's therefore imperative that insurers conduct real-world tests and simulations to battle-proof their well laid plans against practical reality.

Table top simulations offer a good way to test disaster recovery procedures, but to thoroughly understand if the application, database and infrastructure will perform as the disaster recovery documentation states, hands-on technical testing is necessary. However, testing disaster recovery plans in a real-world scenario is no trivial undertaking, and well-designed tests and simulations are time consuming.

A key reason for the expense is inherent in their complexity by design; various skillsets are needed to support a real-world disaster recovery test, and the test may have a direct impact on business operations. These perceived downsides can lead to less frequent testing being approved by the business, which results in blindspots and potential severe vulnerabilities that increase the likelihood of a failed recovery in the event of an actual, real-world outage. A vicious cycle.

Keylane has a no-compromise approach to disaster recovery, and has made full technical disaster recovery tests a standard part of its IT operation (which includes the restoring of both data and reports).

This means that full recovery testing is carried out as often as ten times per year and the outcomes are immediately shared with Keylane's clients. And, as part of its extensive testing, Keylane runs in failover mode for seven days to **guarantee** no disruption to business operations.

Keylane has a no-compromise approach to disaster recovery, and has made full technical disaster recovery tests a standard part of its IT operation.

Cybersecurity measures

With data exfiltration through cyber-attacks such as malware, ransomware and phishing scams becoming increasingly sophisticated and frequent (coupled with the added threat of AI powered attacks raising the stakes considerably), the potential damage against society cannot be overstated. In response to these escalating concerns, **legislators are mandating** that insurers implement and maintain robust and future-fit **cybersecurity measures**.

The majority of insurance companies already have an established first layer of defence, such as firewall protection, antivirus software and intrusion detection systems. Adding to this layer is the deployment of regular security updates, employee training on cybersecurity best practices and, in some cases, red-team vs blue-team exercises.

Dedicated experts are needed to stay ahead of these rapidly evolving threats, but are in high demand and challenging to retain. And, while no foolproof measures exist to 100% protect digital businesses from present and future cyber-attacks, a balance needs to be found that offers a robust level of protection without limiting an insurers' ability to effectively engage with customers and business partners.

Keylane considers cybersecurity to be an **integrated strategic service**. In addition to fundamental measures, Keylane implements more sophisticated countermeasures, which include micro segmented networks, endpoint detection and response/ extended detection and response (EDR/XDR), and an

impenetrable data vault (IDV) that protects data from unauthorised access attempts.

Legacy systems are no longer being secured and kept up to date to the same standard as their modern counterparts.

Regular maintenance and system updates

Keylane runs its software suite on a proven and secure infrastructure, and applying security patches and performing critical updates are treated as critical activities. By following and processing updates based on the latest **Common Vulnerability Security System (CVSS)**, Keylane integrates system updates and maintenance tasks as a standard part of its daily operations.

But, for insurers reliant on legacy systems to run core insurance processes, the reality is less straightforward. Legacy systems are no longer being secured and kept up to date to the same standard as their modern counterparts. Updates are delivered less frequently, and installing them typically requires significant efforts and specialised skills. Complicating things further, many vendors no longer offer support or accept liability on either their platforms or individual legacy components.

This growing disparity forces **legacy dependant** insurance providers down an unsustainable path – pay increasingly higher premium rates for extended support.

And this complexity introduces another negative regulatory impact for insurers to deal with. To support troubleshooting and recovery efforts, the documentation and configuration of all IT systems must be up-to-date as required by regulations and standards. This can be a massive undertaking, and is often time-consuming, multifaceted and resource intensive, especially when an insurer's reliant on external parties.

For its clients, Keylane addresses these issues through 'Infrastructure as Code'. This means that all infrastructure configurations and systems documentation comes with a version control system, and all updates to the environment are fully automated to ensure 100% transparency and consistency.

Understanding incident reporting

From an organisational standpoint it is essential that all employees understand the importance of incident reporting and the correct procedures to follow, such as escalation paths and thresholds.

Next to its extensive training programs, Keylane has implemented well documented processes for incident reporting, including how to deal with defects. These processes dictate when and how to inform a manager, customer or partner, and detail how resolution status updates are to be communicated.

Additionally, several regulations have established requirements to report **significant IT-related incidents** to regulating bodies immediately, including both actual incidents and near miss events that could have

resulted in significant harm. So, insurers must have a clear and comprehensive policy outlining

what constitutes an incident, how incidents should be reported, who is responsible for reporting them, and the timeframe for reporting.

However, a key challenge lies in properly **understanding the impact** of an incident. EU/DORA, for example, has a very clear and specific definition of how an incident must be reported – how many customers were impacted, how much money was lost, etc.


Supporting its clients navigate regulation demands, Keylane provides standard reports for use in reporting to supervisory authorities.

Keylane's ISMS is based on the requirements of ISO27001, of which Keylane is fully certified.

Effective ICT risk management


Another key demand of compliance work is to implement an effective ICT risk management practice. This is an **ongoing process** to detect and respond to emerging threats and vulnerabilities, and requires continuous monitoring of ICT systems and environments.

All insurers must have a documented and well implemented **Information Security Management System (ISMS)**. An ISMS outlines how potential risks and threats to ICT components are identified and prioritised, and supports insurance companies with effective resource allocation based on the severity of a threat.



A common pitfall to avoid here is in allowing an ISMS to become an on-paper only exercise, when it must be something that works in practice. To ensure this doesn't happen, a combination of business process knowledge and technical insight are necessary. However, personnel with these combined skills and experience are few and far between, and a more generalised team with variant skillsets often run into trouble understanding the actual **business impact** of a technical issue.

Keylane's ISMS is based on the requirements of ISO27001, of which Keylane is fully certified. With this in place, the Keylane Risk Officer owns and maintains the Enterprise Risk Management (ERM) process and will, on a quarterly schedule, bring forward and discuss business requirements and evolving risk landscapes that exceed risk tolerances.

 When risks are identified, actions are taken to mitigate risks and reduce the impact. At Keylane, this is part of standard business operations and formalised in the Risk Mitigation Plan.

Complying with data protection and privacy

Compliance work in the context of data protection and privacy involves organisations adhering to relevant

laws, regulations, and standards that govern the collection, processing, storage, and sharing of personal data. Most notably, the General Data Protection Regulation (GDPR) is a legal framework that has changed how organisations handle personal data in the EU.

Axon, Keylane's unified core insurance platform, provides **end-to-end support** for obtaining consent to use personal customer data, be it policy application and in claims registration processes, or strict data governance with regards to managing all privacy sensitive data over time.

When it comes to adhering to GDPR, an important entity is the data controller. The data controller determines the purposes, conditions and means of the processing of personal data. Essentially, they decide how and why personal data is processed.

The client is at all times the data controller, with full responsibility for the measures that protect personal data against unauthorised access, disclosure, alteration, and destruction. The data controller is also accountable for complying with GDPR requirements, and may receive penalties for non-compliance.

Keylane's ISO 27001 certified services guarantee data security for its clients by having a mature information security management system in place, with a proven enterprise risk management process.

This is further outlined in a Data Processing Agreement between the data controller (client) and Keylane.

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) sets clear rules for the collection, use, storage, and transfer of personal data. Non-compliance can lead to serious consequences, including hefty fines, a damaged reputation, and even legal action. This means organizations must take GDPR requirements seriously and work diligently to achieve full compliance.

Axon's insurance platform ensures comprehensive consent management and data governance for personal customer data during policy applications, claims, and long-term privacy.

Stricter outsourcing oversight

The EU/DORA act, effective in the European Union from January 2025, is top of mind for many CIOs.

One reason for this is the changing relationship between an insurer and its relevant outsourcing partners. EU/DORA imposes **stricter requirements** on outsourcing arrangements by demanding that insurers implement a system for monitoring third party

vendor regulation compliance and contractual obligations.

Given the short time until the EU/DORA act becomes effective, many insurance companies are racing against the clock to fill knowledge gaps as quickly as possible – but it's a daunting task, demanding an understanding of contract details, critical outsourcing requirements, regulations, and service **delivery implications** across the entire chain of outsourcing partners.

Keylane's service contracts cover the necessary regulatory requirements. And going further, Keylane strongly believes in having cross-disciplinary sessions, where all aspects of Service Level Agreements are thoroughly reviewed. In addition to all legal obligations, Keylane determines clear monitoring and reporting procedures, and carries out periodic audits, assessments, security controls and performance reviews.

Keylane also provides Service Level Reports, and ISO 27001 certification and ISAE3402 assurance reports. These reports and reviews are essential pillars in the communication between an insurer and auditing parties.

Keylane provides Service Level Reports, ISO 27001 certification, and ISAE3402 assurance reports, which are crucial for effective communication between insurers and auditing parties.

Compliance with confidence

It stands to reason that within the insurance industry, regulation and compliance are vital to ensuring a stable, predictable industry that inspires trust and commitment from policy holders.

With multiple compliance and regulation issues to be aware of at any given time, insurers must take a **business continuity** perspective at all times. But that's no simple undertaking - compliance responsibilities are a daunting task for any insurer, and without the right partner at the helm to help manage and maintain this area of the business, serious problems often arise that restrict an insurer's business agility, accelerate costs, and threaten its reputation.

The most critical element to consider is the insurance core platform (the software and infrastructure). An insurer's core platform sits at the heart of both its business and IT operations as the single most important component in achieving and maintaining regulatory compliance.

But, when running a business on an insurance core platform that is reliant on aging or end of life components, with critical functional dependencies and outdated documentation, any forward looking compliance work becomes a considerable uphill battle. Therefore, when engaging platform vendors for the provision of a new core insurance system, insurance providers must be given the peace of mind that the platform is fully enabled to adhere to **present and future** regulatory requirements.

Additionally, when looking for a **trusted partner** to help navigate compliance, ensure they are aligned with your business and regulatory requirements, risk aware and proactive to cyber-attacks, and above all else have a transparent culture and a proven track record in helping providers succeed in the insurance industry.

A partnership with Keylane

With a proven track record in successful implementations, our dedicated experts, supported by capable partners, work to deliver an ecosystem of emerging technologies that enables Keylane's clients to deliver innovative services and products while driving profit, customer growth and true market innovation.

Headquartered in Utrecht in the Netherlands, Keylane employs around 700 people and delivers services to over 225 insurance companies across the Netherlands, Belgium, Germany, Denmark, Norway and Switzerland.

T +31 88 404 50 00

E info@keylane.com

w keylane.com