

Overspending

*Compliant and Secure without
Overspending by Navigating the
Jungle of Complexity*

Leon Kuhlmann

Nadine Hofmann

Farahnoz Mirboboeva

Victoria Denisiuk

Grey Swan Management AG

July 2024

White paper



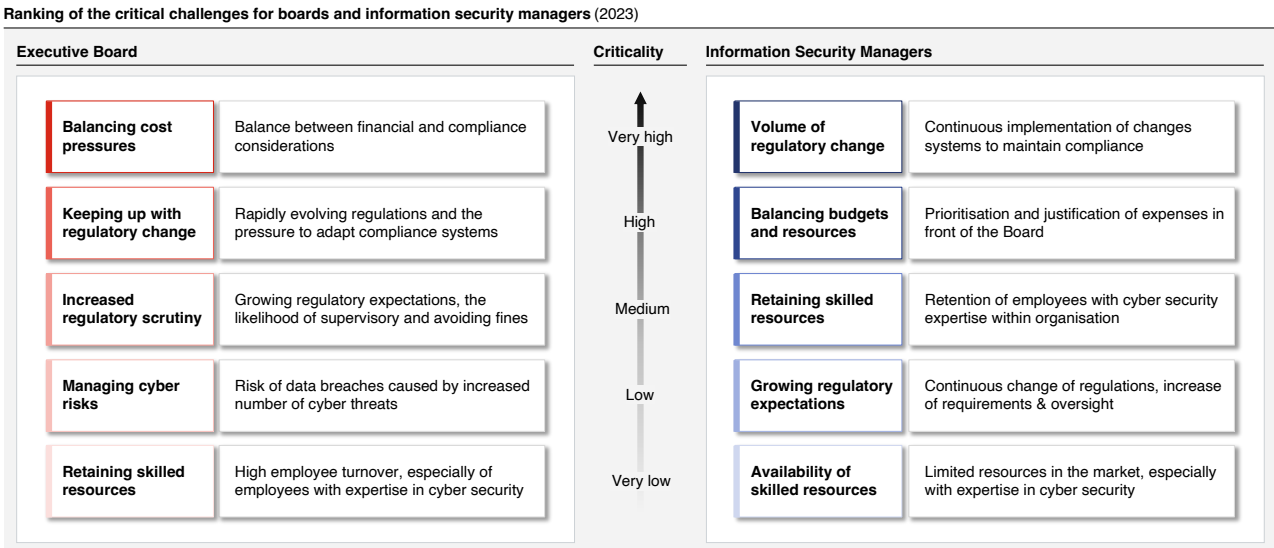
Management Summary

- In today's digital landscape compliance and information security (digital and manual information, cyber and IT) are critical. Navigating the complex regulations and escalating cyber threats demands prioritising adherence to compliance and safeguarding sensitive data to avoid repercussions.
- The CEO and Executive Board are responsible for ensuring compliance and information security (InfoSec) by allocating adequate resources. Due to the consequences of non-compliance and data insecurity, zero-risk biases by the Second Line of Defence and permanent risk presence, companies often opt for solutions with least risk and overspend in the process.
- Regulatory compliance reflected in documents and processes on one side and expensive security measures on the other side do not guarantee the prevention of incidents. The challenge lies in balance: investing in both compliance and security without overspending, while being able to react to evolving threats.
- When it comes to prioritising compliance and InfoSec, a company's strategic approach plays a key role – more innovative, aggressive firms tend to underinvest in these areas compared to their more conservative, defensive counterparts, leading to a misbalanced focus that could expose "attacking" companies to legal, financial, and reputational risks if not addressed.
- New regulations and requirements (e.g., DORA, NIS2, CER) emerging each year and require organisations to stay updated and prepared for an ever demanding regulatory environment.
- Complex IT environments, often a huge mix of custom and third-party, legacy and cloud solutions, require continuous security adaptation, which makes adhering to regulations and security standards increasingly complex as the environment expands and diversifies over time.
- Allocation of dedicated compliance budget is necessary according to the strategic orientation of the organisation to not exploit differently assigned budgets.
- To achieve high-quality, cost-effective compliance and information security, sufficient implementation time is crucial. Regular diagnostics are essential for identifying gaps and preventing incidents. This covers aligning compliance and cyber security requirements with business goals, analysing current capabilities, and mapping a roadmap to the target state, examining strategic and operational aspects. Diagnostics focus on the regulatory landscape, ISMS, cyber security maturity, resilience, vulnerability detection, and testing.

Compliance and Information Security: A Challenging Agenda for the Executive Level

Compliance and information security (InfoSec) is crucial in today's digitalised business world. With the complex regulatory landscape and increasing cyber threats, companies must prioritise adhering to regulations and safeguarding sensitive information to avoid harmful consequences. A data breach, for instance, can cost companies millions of dollars, with the average data breach cost reaching an all-time high of \$4.45 million in 2023. Breaches can cost an average of \$220,000 more when non-compliance with regulations is a factor, increasing this number by 15% over three years.¹

Compliance refers to the processes and procedures that companies put in place to ensure adherence to applicable laws, rules, and standards.² Compliance is complex due to the number of existing legal requirements, constantly changing requirements (e.g., NIS1 to NIS2, CER, DORA) and industry-specific standards (e.g., ISO, NIST, SOC). To comply with them, management systems are a helpful methodology for organisations, such as the internationally recognised ISO 27001 standard for information security to define and implement measures. It defines effective InfoSec as “the preservation of confidentiality, integrity, and availability of information” regarding any handling of information and to safeguard them from incidents such as unauthorised access, modification, destruction, or non-availability.



Source: Grey Swan, Thomson Reuters




Figure 1: *Balancing costs, budgets, and resources is a key challenge*

This white paper elaborates on InfoSec, including IT security and cyber security. InfoSec includes the management of information assets and information systems such as access, usage, disclosure, disruption, modification, or destruction to provide integrity, confidentiality, and availability.³ It encompasses all aspects of protecting information assets and systems including digital and physical. Digital refers to information that can be processed, stored, and transmitted by electronic devices, while physical to tangible objects or environments, including hardware components and paper. Secondly, IT security as a subset of InfoSec, focuses on protecting information technology systems. Thirdly, cyber security covers the protection of systems and networks connected to the internet from cyber threats.

Besides managing the complexity to ensure both, regulatory compliance and InfoSec, it also requires the allocation of adequate resources by executives. The fear of financial, legal or organisational consequences from violations, zero-risk bias of Second Line of Defence (2LoD) stakeholders, and hard-to-challenge agendas can lead to overspending. Consequently, balancing cost pressures is one of the top challenges for CEOs and the Executive Board members, and the second most significant challenge for information security professionals (Figure 1).

Derived from the business strategy, executives and managers generally follow the same overarching goals. However, the importance of certain challenges and their assessment can differ depending on their organisational role and focus. Furthermore, the perspective on cost pressure is not consistently shared across the entire C-suite. Decision making for compliance in general and InfoSec in particular requires involvement of Chief Risk Officers (CRO), Chief Technology or Information Officer (CTO/CIO) Chief Information Security Officers (CISOs) or Chief Compliance Officers (CCO), the 2LoD, as these executives are tasked with ensuring compliance and InfoSec. Although, 2LoD naturally exhibits a bias towards risk avoidance (Figure 2).

The decision drivers of top management regarding compliance topics

Role Driver	Top management roles (selection)						
	CEO ¹	CCO ²	CISO ³	COO ⁴	CRO ⁵	CFO ⁶	CTO ⁷
 Taking ultimate responsibility for company success	Prioritising the company's regulatory compliance	Prioritising the company's InfoSec ⁸ and data protection	Sharing CEO perspective, ensuring compliant operation	Prioritising the company's risk management	Overseeing the overarching financial health	Managing the technological landscape	
 Making ethical, impartial, legally-compliant decisions	Demonstrating strong biases due to the nature of the role	Demonstrating strong biases due to the nature of the role	Prioritising planning and execution of strategic objectives	Demonstrating strong biases due to the nature of the role	No inherent bias, focus on strategic financial planning	Strongly biased to risk avoidance, driven by IT complexity	
 Prioritising secure solutions within time constraints	Proposing a roadmap to adhere to regulatory norms	Advising on a roadmap to enhance security measures	Dedicating time for in-depth topic understanding	Proposing a roadmap to mitigate potential risks	Identifying, assessing, and mitigating financial risks	Impactful role in organisations risk mitigation	
<i>Prejudice</i>	<i>Unbiased</i>	<i>Biased</i>	<i>Biased</i>	<i>Unbiased</i>	<i>Biased</i>	<i>Unbiased</i>	<i>Biased</i>

Source: Grey Swan | 1: Chief Executive Officer, Including Executive Committee | 2: Chief Compliance Officer | 3: Chief Information Security Officer, can include the role of Data Protection Officer | 4: Chief Operating Officer | 5: Chief Risk Officer | 6: Chief Financial Officer | 7: Chief Technology Officer | 8: Information Security

Figure 2:
The distribution of risk avoidance bias in the C-suite

The focus on risk avoidance is often rooted in the potential consequences of compliance violations and possible losses that may extend far beyond just the financial impact. Usually, the incident severity is correlated with the scale: the higher the severity, the more substantial the losses (Figure 3). In cases of low public exposure, the remediation costs for non-compliance are lower, whereas moderate consequences result otherwise in costs three to five times the initial cost. In high severity cases consequences involve legal, reputational, and financial losses, and require mitigations five to ten times more costly. In case of critical level, damage costs and consequences will result in even higher amounts.⁴

For example, the cyber attack on T-Mobile led to the disclosure of personal information for 76.6 million U.S. residents, along with legal and financial consequences.⁵ This included costs related to legal compliance, such as the creation of a \$350 million fund for victims and a \$150 million investment in new security technologies in 2022 and 2023.

Following compliance guidelines does not necessarily mean to be secure by default. In the case of FACC, an aerospace company, hackers orchestrated the theft of approximately €50 million to a supposed acquisition project. The firm sued the former CEO and CFO for \$11 million claiming they failed to protect the company. Moreover, FACC experienced a 17% share price drop due to insufficient information security. Subsequent actions included a revision of internal processes, the full implementation of new security measures, and an intensified cyber security training program for employees at all levels, demonstrating a comprehensive response to the event.



Source: Grey Swan | 1: Categorisation based on the potential risk posed by the incompliance to the organisation's operations or data assets | 2: Business as Usual | 3: Chief Risk Officer | 4: Line of Defense | 5: GlobalSCAPE

Figure 3: Correlation between incident severity and overspending

To illustrate the impressive scale of losses, in 2023 Ireland's Data Protection Commission fined Meta €1.2 billion for violating GDPR by transferring EU user data to the US without proper safeguards.⁵ It is considered one of the biggest fines for violating compliance to date.

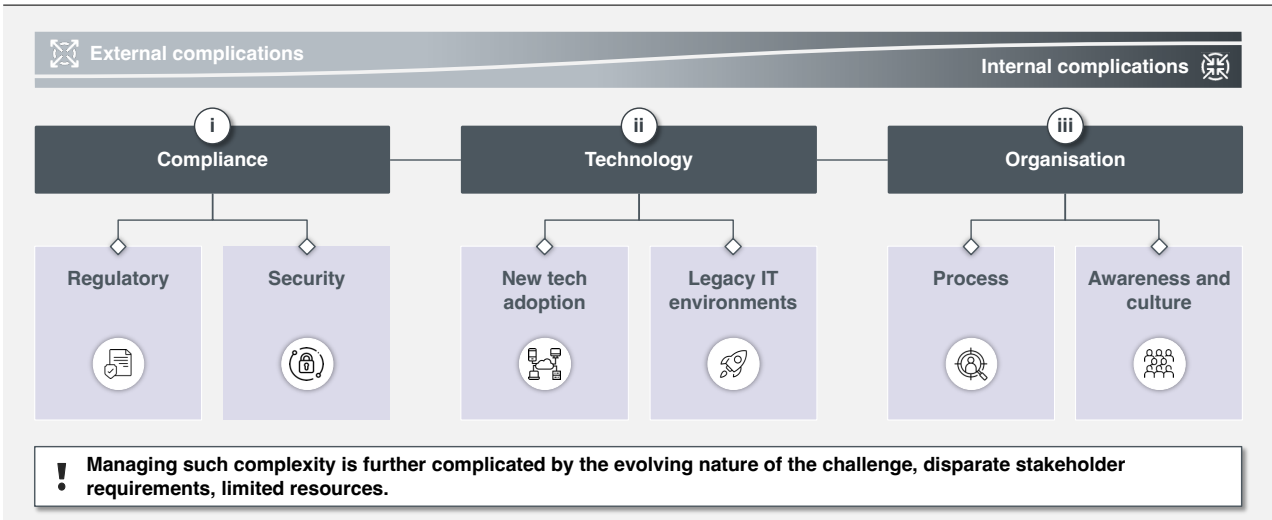
Companies' overspending occurs not only as risk avoidance, but also, in some cases, due to late identification of security gaps. When the current situation on compliance and the state of InfoSec across people, processes, and technology is examined and deficiencies are identified at a later stage, the costs associated with these findings tend to be higher. Three components drive this: first the initial costs of implementing (as a result of insufficient) measures, second the expenses incurred from addressing compliance breaches or security incidents and third – incurred losses.

Unfolding the Complexity

Ensuring compliance and information security is a challenge with external and internal complications for organisations, which can be structured in three complexity areas. Understanding them and their dependencies in a structured approach is key when targeting compliance and InfoSec efforts (Figure 4).

The most immediate aspect in the context of this white paper is the "jungle" of compliance – a set of regulatory and security standards that organisations must navigate. Secondly, navigating technological risks of adopting new technologies and maintaining legacy IT. Thirdly, an often overlooked aspect – awareness and culture underpinned by organisational model and processes.

A high-level decomposition of complexity, without considering market perspective



Source: Grey Swan

This white paper examines why ensuring compliance and InfoSec is a challenge. It tries to create a path in ‘the jungle’ of complexity elaborating on the impact of regulations and security. Beyond ‘the jungle’, the effect of legacy and new technologies as well as organisational settings must be considered to reach high compliance and InfoSec maturity in both directions. Lastly, the publication provides a recommendation on safeguarding organisations without overspending while facing fast developing regulations, cyber threats and technologies. Exec Board can derive appropriate decisions how to allocate budget for compliance measures and programs according to their business strategy.

Figure 4: Executives struggle to challenge compliance and InfoSec because of their complexity

The white paper contributes to a comprehensive knowledge compendium, which analyses the dynamic nature of compliance and requirements, specifically in areas of data protection, cyber security, and regulatory frameworks, among other areas (Figure 5).

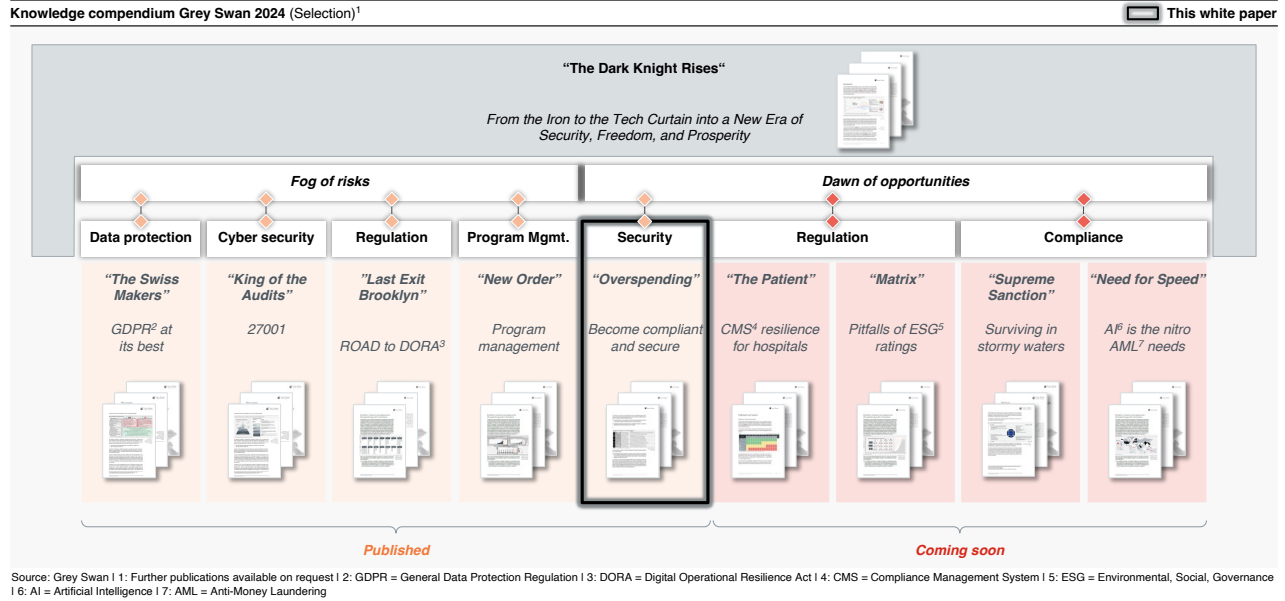


Figure 5:
Grey Swan Knowledge
Compendium 2024

Finding the Right CAPEX Allocation

Cyber threats and information security are key concerns for the C-suite and Executive Board. They must invest in effective security measures to avoid legal, reputational, security, operational, and financial repercussions. As a result, Executive Boards are prioritising information security funding more highly. 93% of CISOs anticipate an increase in their cyber security budgets over the next year.⁶ Prioritising compliance and information security is not merely an expense; it is a cost-saving opportunity.

The challenges become more pronounced on the C-level agenda with the escalating costs of incidents such as data breaches and the corresponding surge in cyber security spending. Costs associated with cyber crime are escalating, with estimates predicting a rise to \$12.4 trillion by 2027 (Figure 6). Critical investments directly impacting compliance and InfoSec should be prioritised within CAPEX of IT budget (Capital Expenditures, long-term investments), emphasising the need to mature those capabilities, not within OPEX (Operational Expenses, ‘day-to-day costs’).

The challenge with this expense lies in CAPEX allocation. In the short term, CAPEX allocation directly impacts the maturity of compliance and information security, necessitating higher upfront investments. However, in the long run, robust information security, proactive maintenance, and regulatory compliance help prevent costly breaches, fines, and remediation. This offsets the higher upfront CAPEX through reduced risk, improved financing, and enhanced stakeholder confidence. With sufficient cash flow, organisations can direct investments into research,

development, and essential long-term measures, subsequently allocating remaining resources for greater shareholder returns.

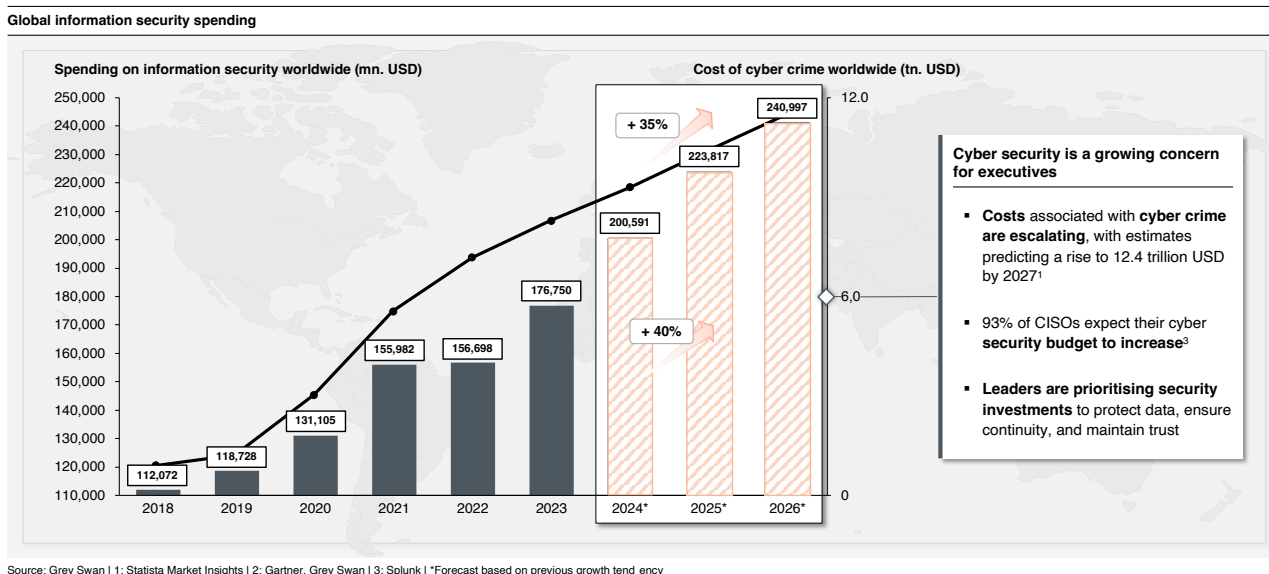


Figure 6:
Cybercrime costs drive
global information
security spending up

Moreover, increasing compliance requirements now consume 40% or more of IT security budgets, risking unsustainable expenses.⁷ This arises from growing compliance and risk frameworks causing duplicated efforts by having redundant controls leading to possible inefficiencies. To optimise, organisations must thoroughly assess their frameworks to identify redundancies. With this, they can then implement lean, tool-supported approaches to compliance, balancing necessary CAPEX investments with more efficient, streamlined processes. This strategic approach helps organisations mitigate cyber risks while maintaining financial sustainability and the ability to invest in growth initiatives.

For early-stage companies, the higher CAPEX (60-70%) allocation over OPEX (30-40%) is crucial for building foundational infrastructure to enable future growth, though it leaves less budget for compliance and InfoSec investments. As the business matures, the balance shifts towards a more even CAPEX-OPEX split, allowing increased spending on compliance and InfoSec to mitigate risks and protect the growing enterprise.

The relationship between CAPEX, compliance, and InfoSec also involves organisational culture – a critical but often overlooked aspect. A strong security culture drives CAPEX in tools and training, however, recognising the centrality of culture and respective CAPEX spend is key to building organisational resilience. Compliant organisations, as exemplified, have demonstrated healthy, successful, and more sustainable business models.

For example, in its early rapid growth, a neobank focuses CAPEX on building a robust digital platform, but overlooks compliance, leading to violations. Later as a mature firm, it is expected that the bank balances CAPEX with OPEX for efficient, sustainable operations that adapt to regulatory changes and customer needs, avoiding the early compliance misstep. For established institutions, like JPMorgan Chase, being one of the biggest investment banks in the USA next to Goldman Sachs and Morgan Stanley, compliance is a critical and ongoing operational necessity. The recurring costs of maintaining compliance are substantial, forming a significant portion of OPEX that outweighs CAPEX.⁸

Balancing CAPEX and OPEX in compliance and InfoSec is crucial for C-level executives to avoid overspending. By prioritising strategic investments in scalable, long-term infrastructure (CAPEX) while optimising recurring operational costs (OPEX) through efficient processes and technologies, executives can ensure robust compliance and security without excessive expenditure.

Higher upfront CAPEX needed to enable robust InfoSec and compliance capabilities, reducing risk and building stakeholder confidence

The Jungle of Compliance

Organisations are facing challenges by keeping up with evolving regulations and security threats. Therefore, it is imperative to understand the nuances and differences of compliance and InfoSec.

The Jungle: Regulation

Regulations are constantly increasing, posing a significant challenge for organisations to comply with. From 2008 to 2016, the average number of regulatory updates per day that typical financial services companies had to manage rose from 10 to an average of 217 regulatory developments.⁹ This exponential increase makes it a top priority for compliance teams to keep up with and react to in a timely manner, as well as to mitigate emerging risks.¹⁰

Regulations can be multidimensional in terms of countries (regional i.e. EU or national), markets (payment), size (anti-monopoly), and infrastructure (critical infrastructure specific). This is challenging especially for organisations operating in multiple countries as it results in increasing costs to manage them. The number of recently published laws show a high need for equal minimum requirements for different regions as illustrated in Figure 7.

Data privacy laws around the world have high focus on protecting personal identifiable information (PII). The EU's GDPR of 2016, requires compliance regardless of location, prompting updates to data exchange agreements. Other regions follow this logic. The UAE's Federal Decree-Law No. 45 (2022) mirrors the GDPR's approach to PII transparency and security. Central Asian countries are also modernising their laws with specifically tailored requirements.

For banks, for example, risk management, incident handling, reporting, and other measures are mandated by prevailing cyber security laws and implicitly or explicitly require an Information Security Management System (ISMS). Over the next months, new laws (e.g., NIS2, CER, DORA) in the EU will be introduced, extending the requirement beyond organisations within the highly regulated critical infrastructure categorisation that become effective in January 2025. The approach to face a number of these challenges is described in Grey Swan's white paper "King of the Audits".

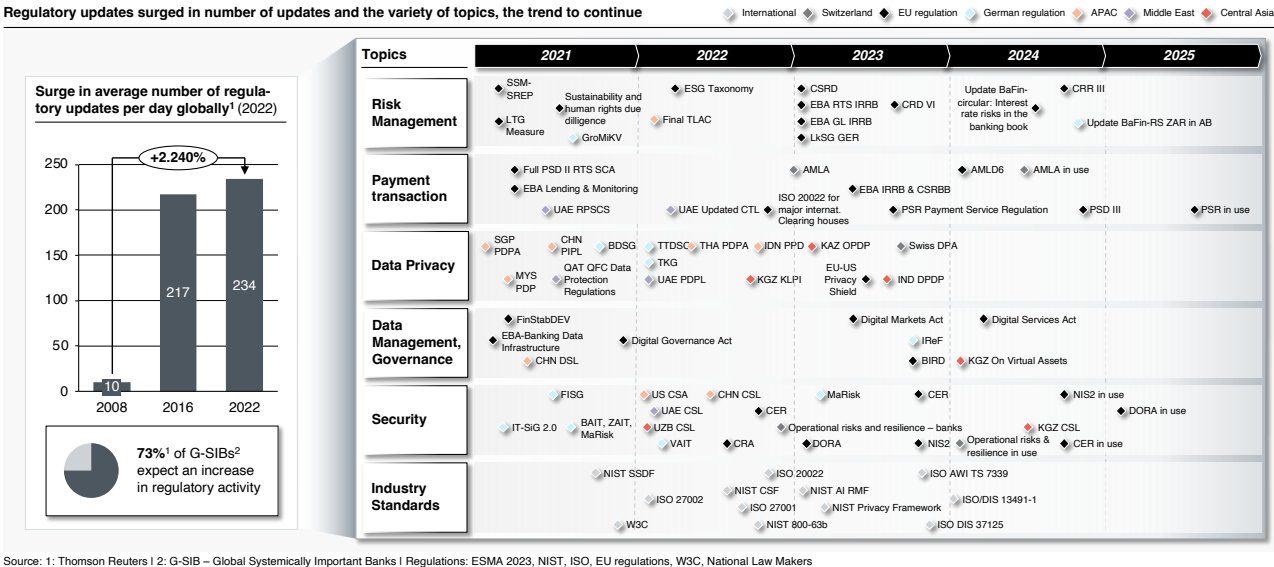


Figure 7: The surge in the volume of regulatory releases and updates

The Network and Information Security Directive 2 (NIS2) establishes requirements for risk management, cyber incident reporting, and implementing security measures. It is expected to impact roughly 160,000 medium-sized and large European companies. Non-compliance could lead to penalties reaching up to 2% of a company's annual turnover.¹¹

The Digital Operational Resilience Act (DORA) focuses on information and communication technology risk management in the financial sector, including service providers. It mandates centralised incident reporting and testing of digital systems. This act will affect over 22,000 financial entities and over 15,000 service providers.¹² Importantly, executives may face personal liability, with fines of up to €10 million. Grey Swan's white paper "Road to DORA" details the steps to meet these requirements.

In parallel with the EU, Switzerland introduced its "Operational Risks and Resilience" framework in January 2024. This framework establishes requirements for certain ISMS components, such as change and incident management, to facilitate cooperation and business dealings with the EU.

As Artificial Intelligence's (AI) impact increases, more jurisdictions and institutions are creating new frameworks or laws establishing a strong foundation for AI development in subsequent years and emphasising ethical considerations (Figure 8).

The U.S. National Artificial Intelligence Initiative Act of 2020 demonstrates a commitment to responsible development through cross-agency coordination and expert committees. The EU followed with the AI Act in March 2024, that focuses on high-risk AI in critical sectors. It requires risk assessments, mitigation measures, usage logs, and human oversight. The Saudi Data and AI Authority established a framework with ethical principles for AI development and technologies.

International organisations are also making significant contributions. The OECD ("Principles of AI", 2019), UNICRI ("Towards Responsible AI Innovation", 2020), and the G7 (Bletchley Declaration, 2023) have published papers promoting cooperation and ethical AI use. The AML specifics are indicated Grey Swan's white paper "Need for Speed".

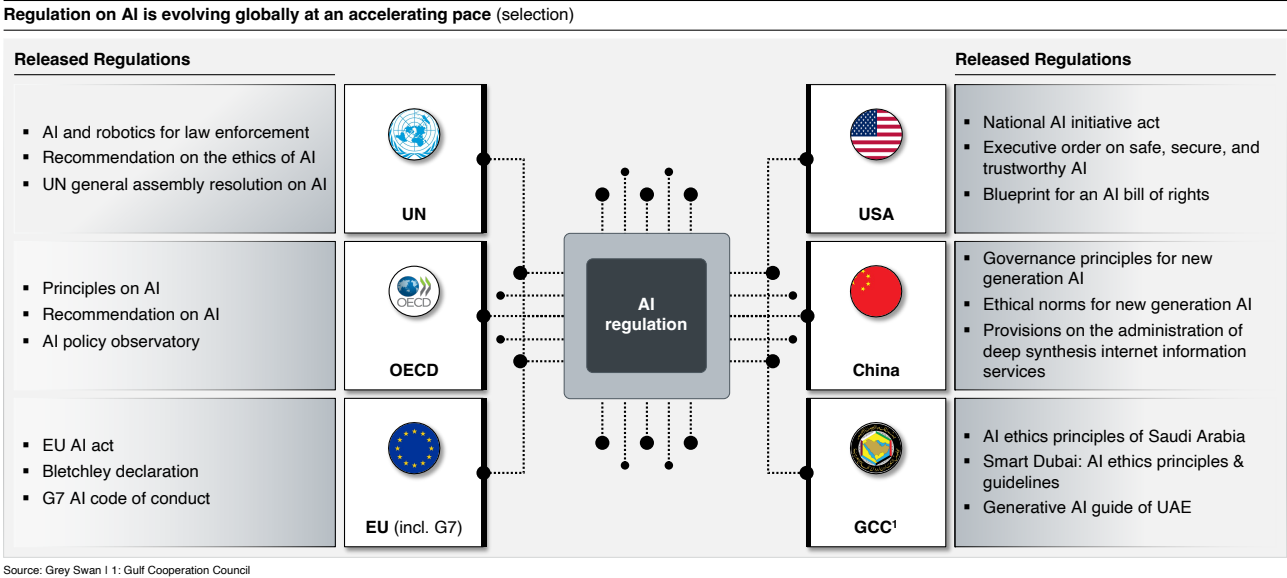


Figure 8: Regulatory developments in data protection, cyber security, AI

Regulations are becoming stricter, with NIS2 and DORA expanding oversight and requirements. Similar trend is to be expected for AI and other laws. This necessitates continuous adaptation of InfoSec strategies for ongoing compliance.

The Jungle: Standards

InfoSec implementation faces the complexity of IT environments and necessity to ensure the right measures and controls addressing IT security and cyber security.

Defining clear requirements and establishing robust security measures is crucial for safeguarding manual and digital information's security objectives confidentiality, integrity/authenticity, and availability (CIAA). These must be fulfilled through various measures along prevention, detection, responding and discovery of cyber attacks:

- **Confidentiality:** Encryption protocols like SSL/TLS of data at rest (storage) and in transfer (transmission between systems, communication channels), identity and access management (access restriction, role-based permission concepts).
- **Integrity/authenticity:** Secure information entry processes, measures against manipulation and tampering, identity, and access management.
- **Availability:** Securing databases, servers, and their recoverability.

Furthermore, when data is no longer needed, secure deletion or destruction is imperative to prevent unauthorised recovery.

IT security describes the protection of information from inside an organisation with regards to processes and tools. Complex IT environments are just like regulations dynamic, often involving a mix of legacy systems, cloud services, third-party applications, and various hardware devices characterised by frequent changes in configurations, updates, and new deployments (and decommissioning).

Cyber security is the protection against threats from outside an organisation, the cyber space (web). To maintain cyber security within an IT infrastructure, regular monitoring of system activities and network traffic is essential for detecting anomalies or security breaches. Periodic audits are conducted to assess the effectiveness of security measures and identify areas for improvement.

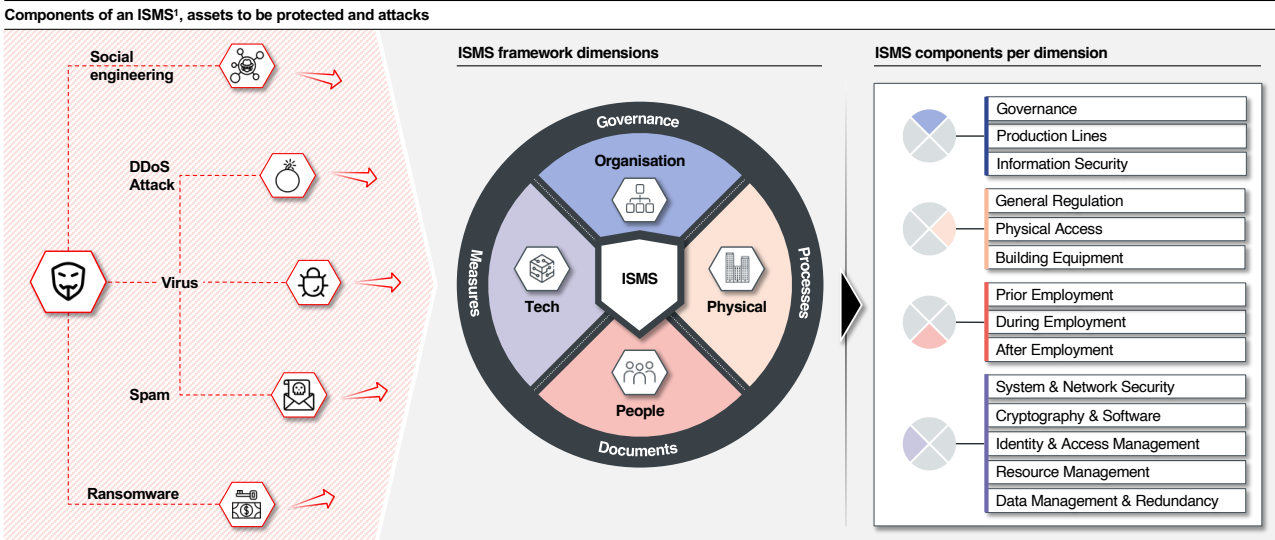
Organisations can leverage a variety of non-binding standards and frameworks for comprehensive InfoSec. Developed by standards organisations or interest groups, these resources provide guidelines and best practices to ensure quality, security, efficiency, and interoperability, which unlike regulations, are not mandatory unless adopted by a regulatory body. Organisations can pick the ideal framework specific to their needs and industry standards.

Known standards, like SOC I / SOC II, NIST Cyber security Framework and ISO 27001, are among the most widely adopted frameworks globally:

- **Service Organisation Control:** SOC I / II are a US-centric certificates. SOC I refers to a service organisation's controls over financial reporting, while SOC II focuses on non-financial controls related to security, availability, processing integrity, confidentiality, and privacy in the cloud.
- **NIST Cyber security Framework:** NIST is a U.S. federal government framework but widely used internationally as a guideline. It provides a policy framework of computer security guidance for organisations to assess and improve their ability to prevent, detect, and respond to cyber attacks. Organisations across industries use it to manage cyber security risk and maintain U.S. government compliance.
- **ISO 27001:** ISO 27001 is a standard that requires specific elements for certification and is internationally recognised. It specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS organisation wide. These controls address various areas, including organisation, physical security, personnel management, and tech (Figure 9). This certifiable approach enhances overall InfoSec, though it requires more time and cost.¹³

Establishing clear security requirements and robust measures is crucial for safeguarding the core information security objectives across both manual and digital data

Choosing a framework requires careful consideration, taking into account the focus of the topic and its applicability. Statistics show that 77% of organisations plan to transition to the latest revisions of applicable security frameworks. In comparison 21% of companies do not intend to act until an audit becomes unavoidable, and some manage compliance manually, which limits their ability to respond to the changing compliance landscape.¹⁴



Source: Grey Swan | 1: Information Security Management System based on ISO 27001

Figure 9: ISMS considered as the best practice for ensuring InfoSec

The global standard ISO 27001 stands out as the most extensive framework for InfoSec, capable of complying with many regulatory requirements and best practices.

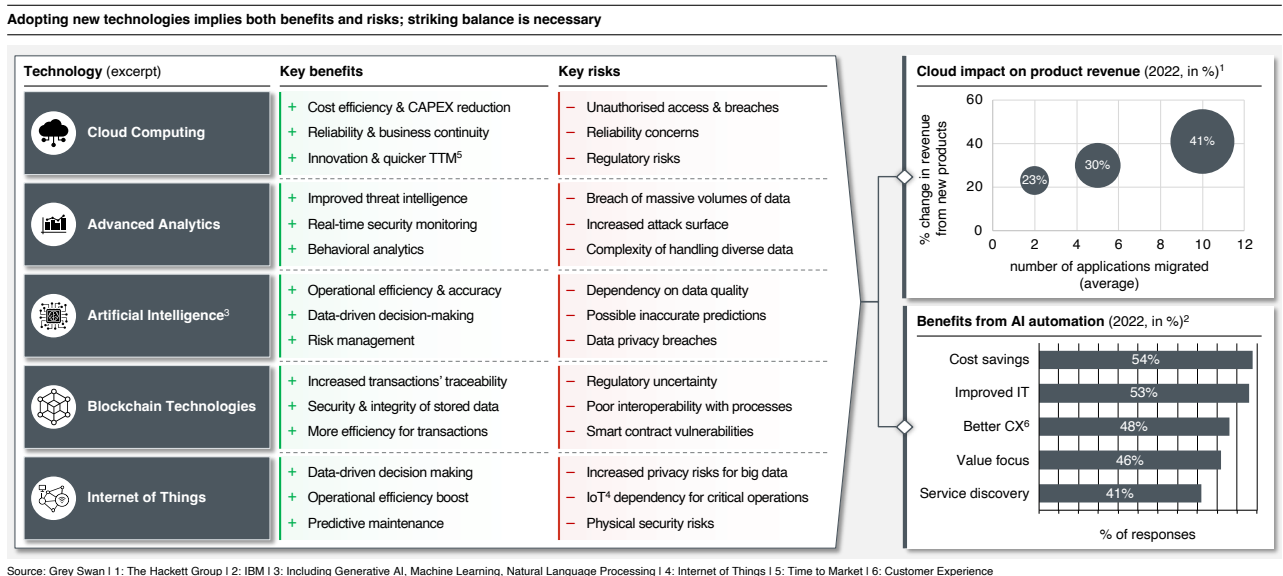
Regulation can necessitate an ISMS, especially as companies' ecosystems expand, since it provides comprehensive and systematic methods to secure corporate information assets (scope depending on the chosen framework) and manage policies, procedures, measures and controls aimed at minimising risks and vulnerabilities. These address various areas, including organisation, physical security, personnel management and technology.

The Tech Dilemma

Having the right systems and tools in place is crucial for ensuring both compliance and information security. In this context, organisations face difficult choices. Firstly, they must decide whether to adopt new advanced technologies, which could increase the risk of non-compliance or expose them to greater data risks. Secondly, they must get upgraded to avoid security vulnerabilities while managing IT complexity and associated risks.

New Technology Implications

Adopting new technologies is essential to remain competitive and meet industry standards and needs. The benefits can be substantial; for instance, modern technology greatly enhances efficiency and productivity through process automation, leading to significant cost and time savings. It also enables advanced data analysis and insights, empowering data-driven decision-making. Additionally, it enhances customer experience, for instance, through personalised interactions (Figure 10).¹⁵ And there is much more to it.



The adoption of new technologies can be risky, as it may introduce compatibility issues with existing systems, scalability challenges, and heightened security and data privacy concerns, particularly as the tools and systems become increasingly interconnected, creating more potential entry points for attackers to leverage and exposing the system to greater vulnerabilities. However, failing technological change can leave organisations behind their competitors and struggling to meet evolving security and compliance requirements.

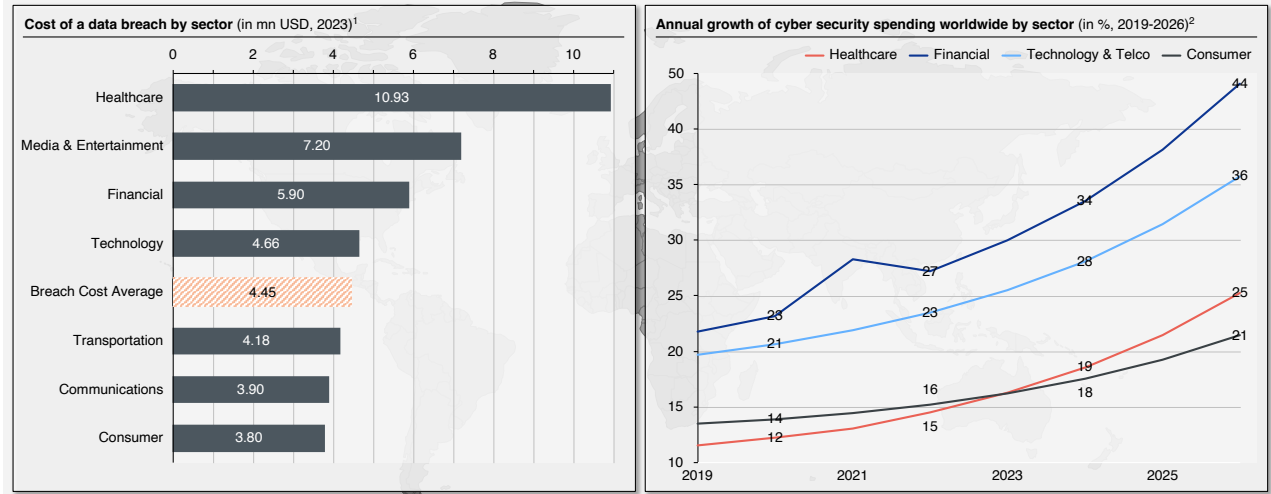
The tech dilemma involves balancing the adoption of new technologies for a competitive edge against the tendency to become risk-averse due to increased complexity, risk exposure, and data risks.

Figure 10: Benefits and risks of adopting new technologies

Examining the dilemma further using the example of AI as a disruptive force, it is estimated that nearly 40% of global employment is exposed to the impacts of AI. This has accelerated the rise of concerns around data privacy, security, and workforce disruption.¹⁶ Moreover, a survey in 2023 of top-level executives and CEOs already found that 21% of respondents identified AI as the leading technology expected to significantly influence their industry in the coming three years.¹⁷

While AI does come with certain security risks, it can also be leveraged to enhance information security and compliance. AI-powered real-time monitoring can detect anomalies in data access patterns, enabling immediate alerting and response. Risk analysis algorithms can identify vulnerabilities and automate incident response procedures while anti-virus programs include AI to increase protection. AI-based user authentication can verify users through behavioural biometrics, enhancing access control. Additionally, AI can be employed to prevent phishing, malware, and other malicious activities by analysing patterns and anomalies.

Highly regulated industries take the lead in cyber security investments, driven by the substantial costs of possible incidents



Source: 1: IBM | 2: European Commission, European Investment Fund, PwC, EIB

Figure 11: Regulated industries lead in cyber security investments

For instance, AI-supported risk profiling can increase accuracy to over 99% by incorporating a variety of data sources.¹⁸ Furthermore, organisations leveraging AI and automation in their security approach reported a 108-day reduction in time to identify and contain breaches, alongside \$1.76 million lower data breach costs.¹⁹

What also contributes to the complexity of staying secure, is that new technologies are also being adopted by cyber attackers. As cyber incidents continue to pose a persistent and significant risk, maintaining AI's position as a leading defensive tool in the digital landscape is crucial. 35% of CISOs are actively experimenting with AI in cyber defence, covering areas such as malware analysis, workflow automation, and risk scoring. The rising professionalisation of cyber crime, coupled with the increasing costs of data breaches, is advancing and reached a higher level of maturity by 2024, especially in highly regulated sectors (Figure 11).

Organisations face more sophisticated cyber attacks, larger attack surfaces, more data to control and increasing complexity in their system infrastructure. In fact, 2023 saw the highest number of cyberattacks with a political intent as geopolitical changes were spiking.²⁰ To address these challenges, organisations are recently turning to AI-driven security approaches and rise cyber security spending as they work to improve their defences.

The evolving regulatory regarding AI necessitates continuous review and adaptation of existing practices to ensure compliance. C-suite executives must undertake a cost-benefit analysis, evaluating the applicability, implementation, and overall value proposition of AI for their specific needs. This proactive approach protects against the impulsive adoption of "the latest" technology, potentially leading to unforeseen downstream issues.

The Legacy

Ensuring compliance and information security in today's complex, heterogeneous IT environments adds to the overall challenges for responsible stakeholders. It demands careful consideration of upgrade and new technologies adaptation, budgeting, and possible risks.

Companies that do not update their IT systems and infrastructure face numerous challenges across entire IT ecosystem (Figure 12). When it comes to security, outdated systems are often less secure and face cyber attacks, as they may not support the latest security patches and protocols. Many companies identified that legacy systems significantly increased their cyber security costs due to the need for frequent patching, updates, or specialised security. 75% of US IT security leaders plan to increase spending on on-premises security upgrades.²¹

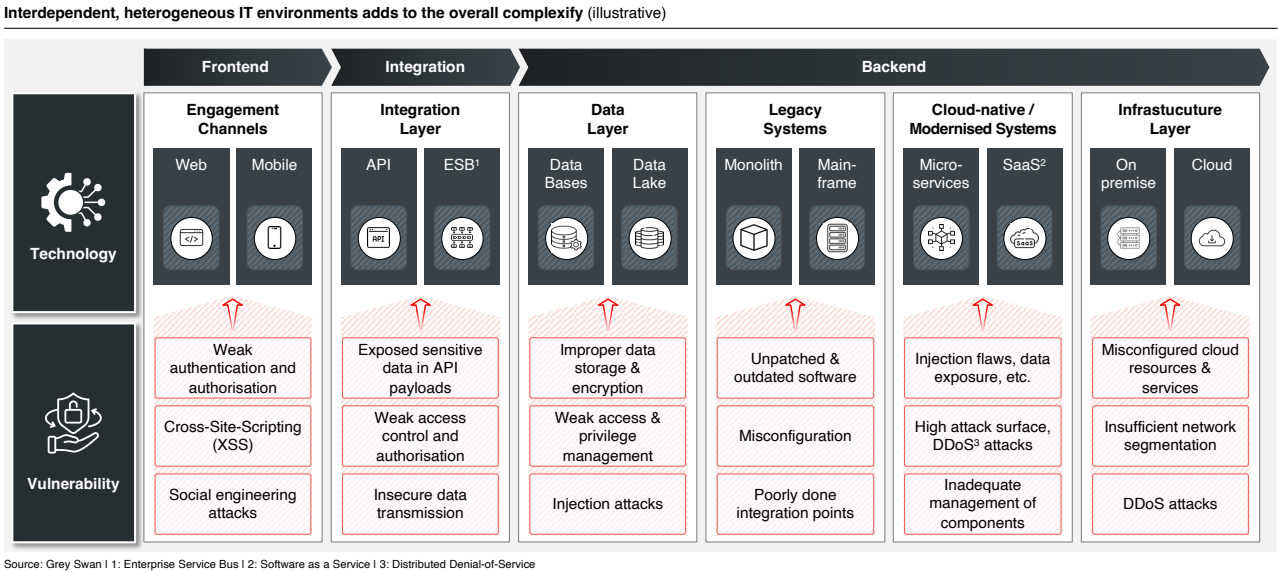


Figure 12: Diverse IT environments increase complexity and vulnerabilities

Additionally, legacy systems can be incompatible with new technologies, leading to inefficiencies and increased maintenance costs. Furthermore, availability of developers and IT experts will decline for legacy software and hardware. In the long run, reliance on obsolete technology likely will lead to fail the company's ability to compete effectively.

Due to the fragmented nature of many organisations' IT environments, which often include legacy systems, cloud services, and various third-party applications, achieving compliance requires complex integration and security measures for these disparate systems. The legacy systems might cause failure to comply with the regulatory standards: over 30% of organisations refer to legacy IT systems as a major challenge to ensure compliance.²²

The tech dilemma in the context of legacy revolves around managing security vulnerabilities, compliance challenges, and operational inefficiencies of outdated technologies, while weighing the costs and complexities of upgrading against the risks of maintaining legacy systems.

Organisations facing this dilemma should prioritise a comprehensive assessment of risks, conduct a thorough cost-benefit analysis, and develop a strategic, phased modernisation plan. This proactive approach can help address security vulnerabilities and compliance gaps while decreasing the costs of migrating to newer technologies.

Organisation: Getting Things Right

The importance of managing the complexity on organisational level can be achieved particularly through processes and culture, especially with regards to compliance and InfoSec, these cannot be overstated.

When considering processes, it is beneficial to think of them as an operating model that fuses together governance, communication, and defined roles/responsibilities. Governance provides the framework to guide decision-making and ensure adherence to policies and regulations. It should align with the company's strategic direction and needs. Effective communication ensures information flows vertically and horizontally.

The human factor is the greatest risk and the hardest factor to control. Well-defined processes act as a safeguard, ensuring consistent actions and reduce mistakes that could lead to breaches or compliance violations. Furthermore, a robust culture can significantly mitigate these challenges which is being fostered by consistently adjusted and improved processes.

In order to effectively implement respective measures, and to establish a culture into organisational structures, it is critical to clearly define and assign roles and responsibilities, and follow principles like segregation of duties, four-eyes-principle or need-to-know, and that are leading by example and create awareness throughout the organisation.

Organisational structure, defined processes, and a security-focused culture are crucial for managing complexity and mitigating human risk

Essential Success Factors in Processes and Skills

Today, the regulator requires organisations to be adequately resourced for an organisation's respective risk profile. Compliance and security talent are crucial for any organisation as they act as the first line of defence against risks and ensure adherence to regulations, protect sensitive data, and mitigate risks through (1LoD) the establishment and following of processes. A strong compliance and InfoSec team mitigates the organisation to a lower risk profile, making the company more attractive to stakeholders.

Moreover, the lack of skilled personnel and low security awareness are the major obstacles, beyond tech hurdles, when it comes to ensuring compliance and InfoSec (Figure 13).

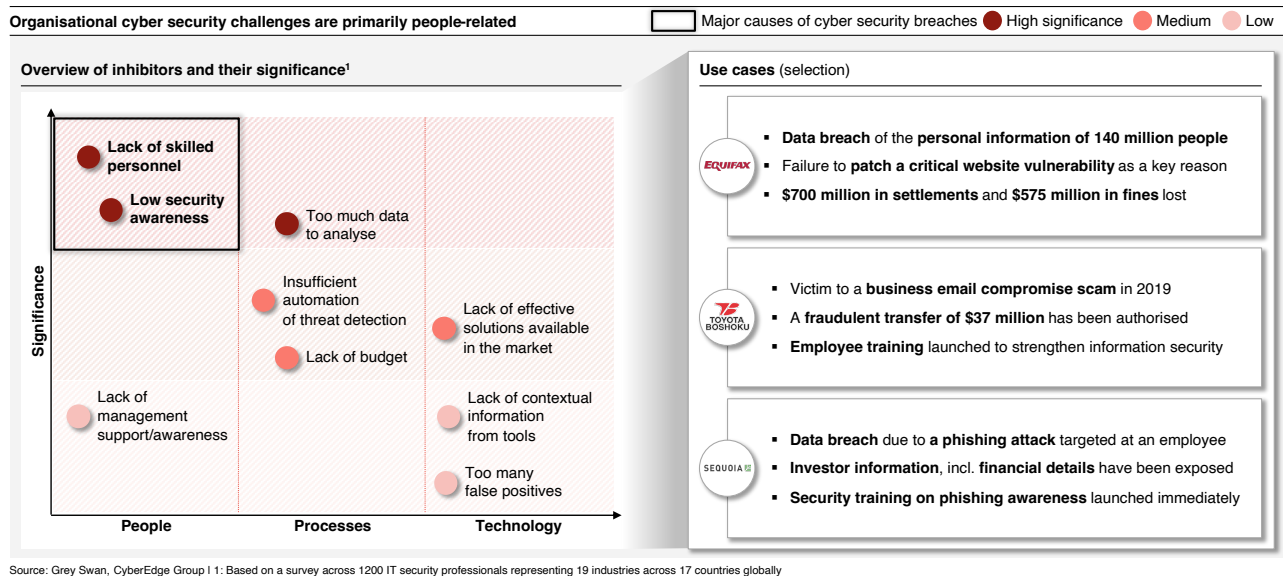


Figure 13: Effective InfoSec heavily depends on the right culture

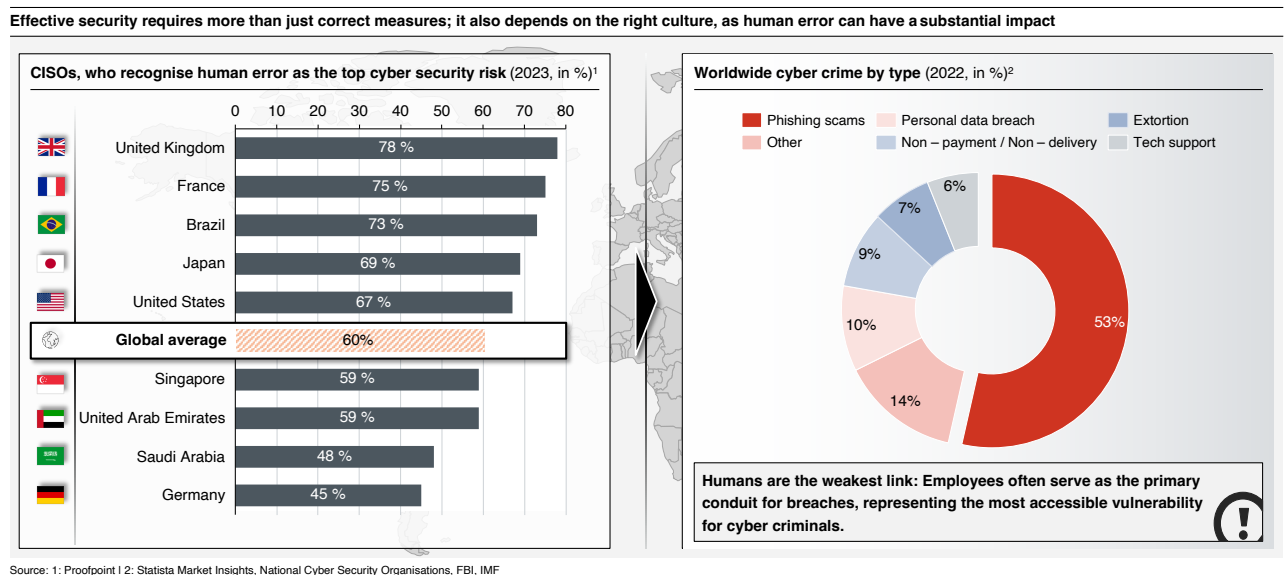
Maintaining compliance and InfoSec requires a diverse set of experts with specialised skills and knowledge:

- **Compliance Officer:** Develops and implements compliance policies and conducts audits to ensure adherence to regulatory requirements.
- **Chief InfoSec/Data Privacy Officer:** Ensures compliance with cyber security/privacy laws, manages policies, evaluates management system performance, and consults to incidents.
- **Risk Management Officer:** Identifies and assesses risks, develops risk mitigation strategies, ensures alignment with compliance standards and the organisation's own risk framework.
- **Cyber Security Analyst:** Monitors and analyses security threats and alerts as well as implements following security measures.
- **Incident Response Team:** Handles security incidents, coordinates cross-departmental problem-solving, ensures proper documentation, and follows up on changes and improvements.

The responsibility for cyber security and compliance can fall on various roles, such as the CIO, CISO or DPO, who then interact with the Exec Board on these matters. This growing focus on cyber security is reflected in the rise of CISOs, with 47% now reporting directly to their CEOs.⁶ Organisations must invest in these essential positions to address challenges as each role of the 1LoD and 2LoD contribute uniquely to uphold regulatory standards, develop risk mitigation strategies, assess cyber security threats, and manage data privacy. While the 1LoD executes actively the processes to run the organisation, 2LoD per definition executes controls to ensure the correctness of the processes and otherwise corrects them to improve the effectiveness and stability of these. Companies known for their high level of cyber security maturity have increased the number of cyber security specialists by up to 10% of their total IT workforce in 2022.²³ The growing significance of these roles is reflected in the escalating costs to hire and retain such specialised talent.

The Crucial Role of the Awareness and Need for Culture

The cultural aspect and the impact of human behaviour are often overlooked in organisations. Significant potential for failure resides with employees, often leading to security breaches. At least half of the CISOs interviewed worldwide acknowledge the human error as the biggest cyber security vulnerability (Figure 14).



Selected key human factor challenges that pose significant risks to organisations include:

- **Phishing attacks:** Despite having regulations and trainings in place to prevent phishing, studies have shown that up to 20% of employees sometimes still click on malicious links. 82% of data breaches in 2023 were caused by social engineering using the human factor as a vulnerability.²⁴ Another source indicates that the human element accounts for most incidents (74% of total breaches), despite efforts to safeguard critical infrastructure and increase trainings. This highlights the difference between knowing vs. doing it effectively.²⁵
- **Low staff morale:** Recognised as a significant risk, potentially can lead to broader non-compliance issues through errors or manipulation. The high level of cyber threats highlights where security measures may hinder a business's agility. Addressing this challenge requires understanding that information security is more of a cultural issue than a technical one. Culturally, information security awareness must be integrated across all organisational levels. To foster a security-conscious mind-set, trainings and raising awareness are key.
- **Lack of skilled personnel:** At the management level, transitioning to a digital-first approach requires skilled personnel and a shift in security practices to make everyone responsible for cyber security. This emphasises a "security as a code" mindset, underpinning the belief that people will only prioritise the right actions when they genuinely care. This leads to implementation of technological and procedural changes, although the introduction of new methods may encounter resistance that requires careful overcoming.

When the management demonstrates a strong commitment, it will set a tone for the whole organisation, encouraging a culture of compliance and InfoSec awareness. Employees are more likely

Figure 14:
Effective security needs
both strong measures
and a culture

to adhere to necessary protocols and processes when being informed, engaged and involved into an aware environment for their necessity. Otherwise, this will lead to a lack of appropriate reporting and oversight. This can result in risks such as regulatory penalties, security breaches, and financial losses.²⁶

Managing the Hard-to-Manage Reasonably

High-budget campaigns for compliance and InfoSec will likely fail without clear goals, lack in understanding of (information) assets, low numbers of implemented controls and becoming a key reason for overspending.

There is no straightforward or one-size-fits-all solution that will guarantee full compliance, maximum InfoSec, and optimal spending. Regulation does not create entirely new security measures for each law. Instead, it establishes a strong baseline, requiring organisations to implement step-by-step improvements to achieve compliance and security across all aspects of their operations.

Without understanding the risks, organisations cannot determine if they are allocating adequate amount of resources to protect themselves. Due to missing, incomplete or incorrect empirical performance data, the effectiveness of the security measures cannot be quantified.²⁷ Ignorance, on the other hand, masks the real risk profile, leading to a focus only on high-level risks.²⁸





Moreover, considering an organisation's strategy is essential for ensuring the appropriate approach to handling complexity and ensuring adequate allocation of resources:

- **Ignore:** Involves consciously choosing not to respond to competitive threats or market changes, focusing on stability in established markets. Companies adopt this approach when they believe threats are insignificant or their core strengths, and their market position is robust enough to withstand potential impacts.
- **Defend:** Focuses on maintaining market position and safeguarding the existing customer base against competitive threats. It achieves this through continuous improvements that reinforce the organisation's strengths and fortify its defenses against potential attacks.
- **Attack:** Aggressive approach which prioritises achieving market dominance through competitive actions. It involves proactive and often bold strategies to capture market share, attract customers, or undermine competitors.
- **Design:** Centered around innovation, creativity, and user-centric approaches to develop unique products, services, or experiences, thus shaping new markets. This strategy emphasises the importance of design thinking in achieving competitive advantage.

There is no one-size-fits-all spending solution for ensuring Compliance and InfoSec, but proactiveness to understand the risks and gaps should be universal

Figure 15 categorises approaches for organisations in established versus new markets, dividing their focus areas into compliance, technology, and organisation. The key takeaway is that the priorities of organisations across these categories differ depending on the chosen strategy. Companies in established markets, particularly those with "Ignore" and "Defend" strategies, prioritise protecting their market position. This focus can lead to overlooking emerging trends and technologies. However, as a trade-off, these companies often have a strong compliance baseline and established information security systems.

Solution framework based on the strategy style of the company

Lever		Established Market			New Market
		Ignore 	Defend 	Attack 	Innovate 
Compliance	Regulatory	High focus, recognising criticality of incompliance to market position	High focus, implementing proactively risk assessments , controls and audits	Low focus, directing all efforts on hyper-scaling	Low focus, all organisational effort directed at continuous innovation
	Security	High focus, recognising criticality of security breaches to market position	High focus, proactive identification and control of vulnerabilities	Low focus, only critical tech adopted to eliminate vulnerabilities	Low focus, advanced tech, incl. enhanced security tech likely in place
Technology	Emerging	Low focus, adoption only when necessary due to potential disruptions	Medium focus, adopting new tech only when the benefits outweigh the risks	High focus, continuous adoption especially if high impact on growth	High focus, ongoing adoption, self – innovation and investments on R&D
	Legacy	High focus, fortification of legacy systems due to complexity and risks	Medium focus, modernising only core systems & using integration solutions	Low focus, most likely to leverage only advanced tech to enable scalability	Low focus, most likely to leverage only advance tech to enable innovation
Organisation	Process	High focus, embedded operating model , changes occur only if critical	High focus, established operating model and assigned talent	Medium focus, partially formalised operating model and dedicated talent	Medium focus, R&D-centric operating model , partially dedicated talent
	Culture	Low or no focus, most likely to have a risk-averse culture	Medium focus, fostering a culture that balances innovation with stability	High focus, promoting a culture of agility to ensure speed and scaling	High focus, cultivating a mission – driven culture to enable novelty
Market distribution		2.5%	95%	2.5%	

Source: Grey Swan

Figure 15: Solution framework aligned with the company's strategic approach

Conversely, companies targeting new markets focus primarily on innovation, leveraging advanced technologies, and fostering a culture of agility, but may lack the robust security posture of their established market counterparts.

Even if targeting established markets, organisations with the "Attack" strategy prioritise new technology, talent, and agility, allowing them to remain flexible and responsive to swift changes in the market (Figure 16). Legacy infrastructure receives moderate investment to ensure functionality, while compliance and risk management are deprioritised as rapid growth is more of a priority.

The usual approach companies take in both markets can backfire. Companies with "Ignore" or "Defend" strategies, risk overspending on compliance. Conversely, "Attack" or "Innovate" strategies may expose companies to costly regulatory fines, data breaches, or security incidents that can exceed the upfront investment in compliance.

Dedicating an adequate portion of financial resources to compliance and InfoSec is a strategic decision that ensures long-term financial stability and operational integrity. By investing in these critical areas early on, companies can mitigate the risks of regulatory fines, data breaches, and security incidents.

For companies with "Innovate" or "Attack" strategy, this is especially crucial as they are often more vulnerable to such risks due to limited resources and evolving infrastructures. They also need to build trust with customers and stakeholders, and demonstrate a commitment to robust compliance and InfoSec measures that can provide a long-term competitive advantage.

Companies with "Ignore" or "Defend" strategies risk overspending on compliance. To avoid this, they should evaluate whether all their compliance measures are effective and truly necessary. Ineffective measures only provide a false sense of security, potentially exposing them to even greater financial risks later.

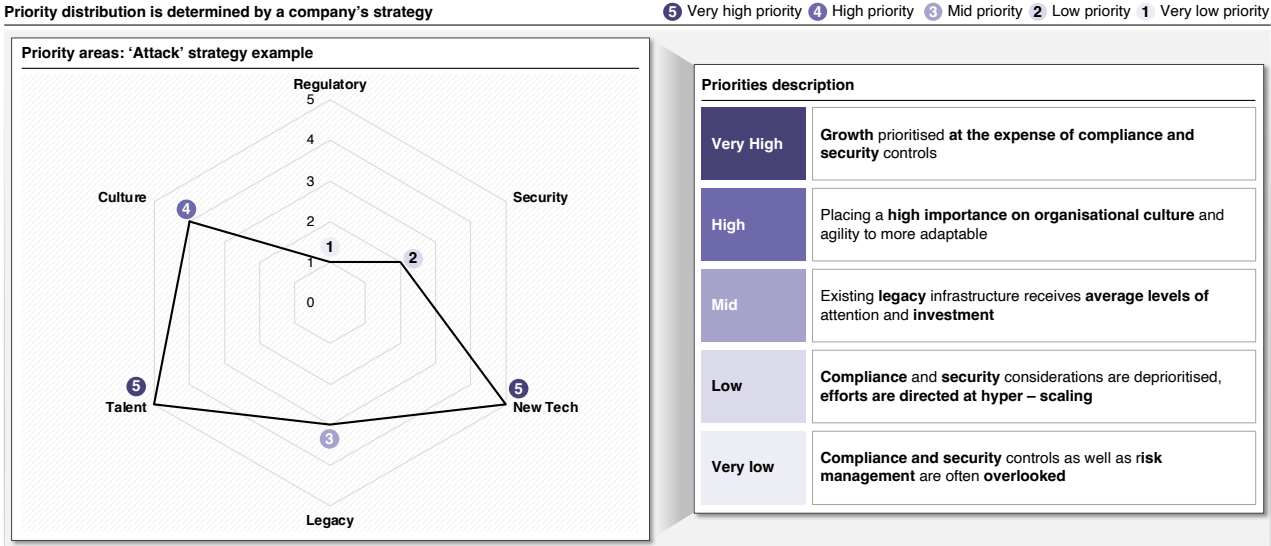


Figure 16: Company strategy impacts compliance priorities

Figure 17 provides an analysis of budget allocation across various strategies and the corresponding regulatory risks.

A well-structured diagnostic approach is a good starting point for an early detection of compliance and InfoSec gaps that can incentivise management to take action and avoid higher restructuring costs later. It is also crucial to maintain a balanced and unbiased approach, ensuring a neutral evaluation of the security practices. An assessment of an organisation's compliance and InfoSec state can identify gaps with which the right actions can be planned and implemented. Only with a clear knowledge on what to do organisations can prevent under- or overdelivery. Companies must proactively address identified security gaps using reasonable resources and effective management. Failing to do so risks significantly higher costs from reacting to future security incidents.

In order to tackle the challenges in a smart way, it is necessary to start with a two-step gap analysis per respective use case (compliance, including management systems and IT security setup, or cyber security) always looking at the deviations that must be closed and that describe the efforts on one hand, followed by how to close these on the other hand.

When it comes to compliance, the first step is **regulatory efforts navigation**. The initial phase focuses on understanding the regulatory requirements specific to the organisations, including anticipating upcoming regulatory frameworks and standards. Next, an evaluation of the potential impact of funnelled regulations on the operations, systems, and data is conducted. Crucially, gaps are identified against current measures and controls, and provide recommendations for new actions, ensuring a clear understanding of their implications for the company and projecting efforts accordingly.

The subsequent second step is the **health check for compliance & InfoSec** phase that is designed as a discovery of current capabilities, followed by proposing new structures. It starts with

defining the target state for achieving compliance and proceeds to identify and map non-/compliance areas specific to a framework, providing visibility into misalignment areas. It concludes with developing a roadmap for essential compliance measures tailored to a specific framework.

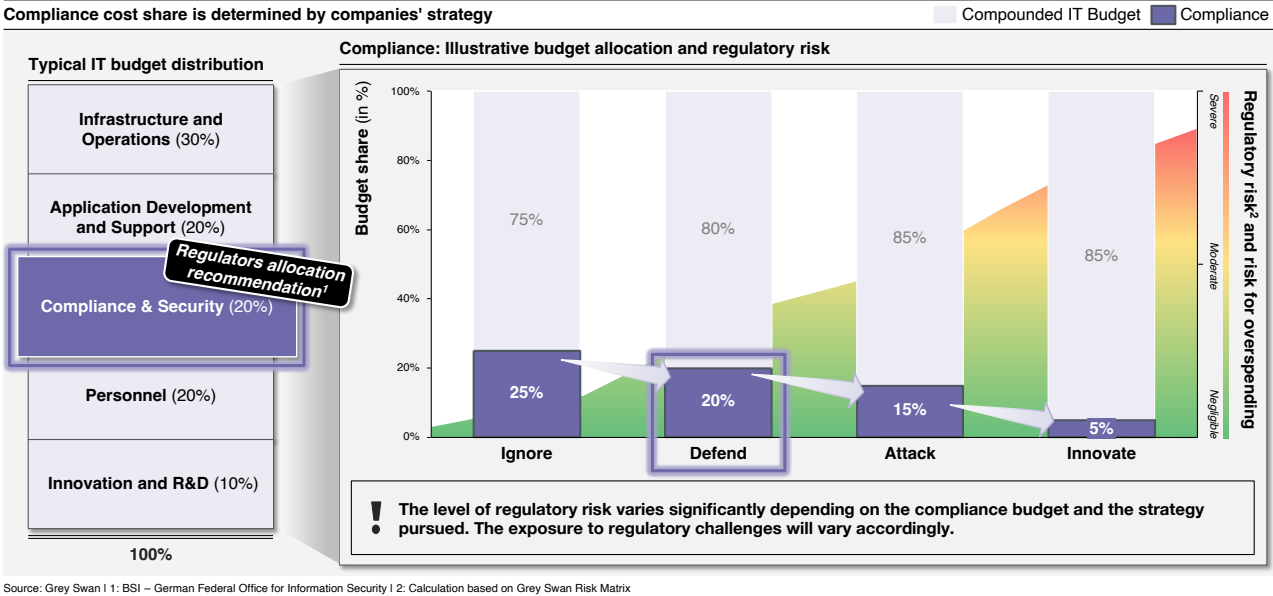


Figure 17:
Lower compliance and InfoSec budgets increase overspending risk

When it comes to cyber security, **security diagnostics** rely on understanding the maturity of an organisation's existing cyber security capabilities. The results of the discovery process, along with the cyber security vision, should be aligned with the broader business strategy. It provides crucial visibility into current vulnerabilities and assesses their severity.

The first step is **strategic analysis** that evaluates an organisation's capabilities in safeguarding against cyber threats and provides a diagnosis of cyber security risk management practices. This combined evaluation enhances visibility into risk readiness, identifies gaps, and ensures the cyber security strategy aligns with the overall business strategy.

The second step is **technical analysis** and is a hands-on exercise that constitutes the audit of processes and technical environments, including penetration testing of both public-facing and internal infrastructure. The primary goal is to gain visibility into risk exposure, analyse the impact of discovered vulnerabilities, and propose effective remediation measures.

The results of the diagnoses, taking into account the company's business strategies, show the focus that needs to be driven forward (among others): the realisation of the company's own compliance situation, the need for the necessary specialist personnel, the reinforcement of insufficient measures, or new concrete measures. Prioritising them helps to focus on the most pressuring subjects at hand and to mitigate the greatest threats first.

When it comes to processes, regularly reviewing routines and procedures is vital to ensure they remain effective and up-to-date. The review process should identify any weaknesses or outdated practices, allowing for continuous improvement and ensuring the organisation is always prepared to handle threats efficiently. Additionally, maintaining a robust network of contacts with regulatory and security authorities is essential. These relationships can provide timely assistance, advice, and support when dealing with threats. They also ensure that the organisation stays compliant with legal requirements and benefits from the latest security insights.

Regarding company's culture, clear communication and protocols are to ensure that all team members understand the risk of non-compliance and security violations. Management commitment can be counted on the basis of compliance communication. Training, awareness measures and setting the "tone on top" as well as the motivation for direct managers for the "tone in the middle" can be implemented and measured. It ensures a common understanding throughout the organisation and prevent misconduct.

In summary, achieving the "holy trinity" of speed, quality, and cost simultaneously is impossible. Based on experience, only two of these three can be prioritised at once. Therefore, if the goal is to achieve high quality (compliance and InfoSec in this context) on reasonable costs, sufficient time must be allocated.

The diagnostic framework covers two aspects (compliance and cyber security) and two levels (strategic and operational)

Summary

This white paper examines the critical importance of compliance and information security (InfoSec) for today's digitalised businesses. With escalating cyber threats and an increasingly complex regulatory environment, organisations must prioritise adherence to regulations and protection of sensitive information to avoid severe repercussions.

CEOs and Exec Boards are ultimately responsible for ensuring compliance and InfoSec, necessitating them to ensure adequate resources with the right skill sets to enable informed decision making, and balancing the high costs of measures with the need for financial sustainability. Otherwise management bears the risks for overspending which is high due to the severe consequences of non-compliance and data breaches and not knowing the necessary gaps to avoid these.

Regulatory and security standards form a jungle of constantly evolving new laws or updates of them with increasing numbers. Internationally operating companies face additional challenges due to overlapping and evolving regulations. Simply complying does not guarantee true protection. Organisation must go beyond the "checkbox" mentality and prioritise the effective implementation and execution of security measures. Frameworks that supposedly provide guidelines for maintaining high InfoSec standards but can also form a trap of doubled requirements that are not identified for merge and therefore result in double costs.

The adoption of latest technology can enhance efficiency but also increase risks and complexities due to the historic growth of the IT environment. Outdated technologies pose significant security vulnerabilities and compliance challenges – relating to overspending issues.

This is why organisations need reliable processes to steer effective governance, communication, and a strong security culture are essential for maintaining compliance and InfoSec. With the right roles and responsibilities, clear definition and assignment of roles (e.g., Compliance Officer, CISO, Cyber Security Analyst) are critical for effective risk management.

For ensuring Compliance and InfoSec there is no "one-size-fits-all" solution. Organisations need to take into account the jurisdiction, business model, operational setup, and cost efficiency of their compliance expenditures. They need to prioritise investments in compliance and InfoSec to ensure long-term operational integrity and financial stability.

Organisations that tend to overspend on compliance should ensure that their measures are genuinely effective to avoid a false sense of security and increased financial risks. Companies that focus on innovation should prioritise compliance investments to mitigate risks and build trust with customers and stakeholders, thereby gaining a long-term competitive advantage.

To achieve this, organisations should conduct a thorough and well-structured diagnosis to identify critical areas for improvement. Establishing a neutral function to challenge proposals can help prioritise improvements and prevent overspending, ensuring alignment with strategic business goals.

Sources

1. IBM Corporation. (2023). *Cost of a Data Breach Report 2023*. Retrieved from <https://www.ibm.com/downloads/cas/E3G5JMBP>
2. Brooklyn Journal of Corporate, Financial & Commercial Law. (2016). *Compliance, Technology, and Modern Finance* article. Retrieved from *Temple University Legal Studies Research Paper No. 2017-06*.
3. US National Institute of Standards and Technology (NIST). (n.d.). *INFOSEC - Glossary / CSRC*. Retrieved from <https://csrc.nist.gov/glossary/term/INFOSEC>
4. GlobalSCAPE Inc. (2017). *GlobalSCAPE, Inc. and Ponemon Study Finds Data Protection Non-Compliance Expenses*. Retrieved from <https://www.globalscape.com/news/2017/12/12/globalscape-inc-and-ponemon-study-finds-data-protection-non-compliance-expenses-45#:~:text=GlobalSCAPE%2C%20Inc.,and%20Ponemon%20Study%20Finds%20Data%20Protection%20Non%2DCompliance%20Expenses%20Up,Costing%20an%20Average%20%2414%20Million>
5. CSO (from Foundry). (2024). *The biggest data breach fines, penalties, and settlements so far*. Retrieved from <https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>
6. Splunk. (2023). *Emerging trends, threats and strategies for today's security leaders*. Retrieved from The CISO Report.
7. Coalfire and Omdia. (2020). *Cyber Report: Compliance Burdens Unsustainable*. From Coalfire website. Retrieved from <https://coalfire.com/insights/news-and-events/press-releases/2020-cyber-report-compliance-burdens-unsustainable>
8. Finbox. (2023). *EBITDA - CAPEX for JPMorgan Chase & Co*. Retrieved from https://finbox.com/NYSE:JPM/explorer/ebitda_less_capex/
9. Thomson Reuters. (2023). *Cost of Compliance Report*. Retrieved from Thomson Reuters Regulatory Intelligence.
10. Thomson Reuters Institute. (2023). *Risk & Compliance Report*. Retrieved from Thomson Reuters Institute.
11. EQS Compliance COCKPIT. (2024). *The Biggest GDPR Fines of 2023*. Retrieved from <https://www.eqs.com/compliance-blog/biggest-gdpr-fines/#:~:text=with%20European%20regulators.,In%20summary,which%20amount%20is%20higher>.
12. PwC UK. (n.d.). *DORA and its impact on UK financial entities and ICT service providers*. Retrieved from <https://www.pwc.co.uk/industries/financial-services/insights/dora-and-its-impact-on-uk-financial-entities-and-ict-service-providers.html>
13. Grey Swan analyses different frameworks with regards to their applicability, scope and certifiability in the whitepaper "Transformation of the regulatory world".
14. Coalfire. (2023). *Securealities Report: 2023 Compliance*. Retrieved from <https://coalfire.com/insights/resources/reports/securealities-report-2023-compliance>
15. NorthRow. (2023). *10 reasons why you should be using compliance data in your budget planning for next year*. Retrieved from <https://www.northrow.com/blog/why-you-should-be-using-compliance-data-in-your-budget-planning-for-next-year>
16. International Monetary Fund. (2024). *AI Will Transform the Global Economy. Let's Make Sure It Benefits Humanity*. Retrieved from <https://www.imf.org/en/Blogs/Articles/2024/01/14/ai-will-transform-the-global-economy-lets-make-sure-it-benefits-humanity>

17. Gartner. (2023). *Gartner Survey Finds CEOs Cite AI as the Top Disruptive Technology Impacting Industries*. Retrieved from <https://www.gartner.com/en/newsroom/press-releases/2023-05-17-gartner-survey-finds-ceos-cite-ai-as-the-top-disruptive-technology-impacting-industries>
18. ShuftiPro. (2023). *Understanding EKYC | The Benefits, Processes & 2024 Forecast*. Retrieved from <https://shuftipro.com/blog/understanding-ekyc-the-benefits-processes-2024-forecast/>
19. IBM. (2023). *Cost of a Data Breach Report 2023*. Retrieved from <https://www.ibm.com/reports/data-breach>
20. Statista. (2023). *Annual number of cyber incidents with a political dimension worldwide from 2014 to 2023 YTD*. Retrieved from <https://www.statista.com/statistics/1428487/number-political-intent-cyberattacks-annual/>
21. Forrester. (2023). *Planning Guide 2024: Security And Risk*. Retrieved from *Forrester Vision Report* https://go.forrester.com/wp-content/uploads/2023/07/Planning-Guide-2024_Security-And-Risk_.pdf
22. Capgemini. (2019). *Championing data protection and privacy – a source of competitive advantage in the digital century*. Retrieved from https://www.capgemini.com/wp-content/uploads/2019/09/Report_Championing-Data-Protection-and-Privacy.pdf
23. Bain & Company. (2022). *Building Strategic Cybersecurity Capabilities After the Invasion of Ukraine*. Retrieved from <https://www.bain.com/insights/building-strategic-cybersecurity-capabilities-after-the-invasion-of-ukraine/>
24. Verizon. (2023). *Data Breach Investigations Report: Top Takeaways*. Retrieved from <https://www.verizon.com/business/resources/reports/dbir/>
25. Verizon. (2023). *Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket*. Retrieved from <https://www.verizon.com/about/news/2023-data-breach-investigations-report>
26. Compliance Next by CREATE Compliance. (n.d.). *The Top 10 Reasons Compliance Programs Fail*. Retrieved from <https://www.navexglobal.com/compliancencnext/media/doc/Top-10-reasons-compliance-programs-fail.pdf>
27. SightGain. (2023). *Investing in cybersecurity: are you overspending or underspending?* Retrieved from <https://sightgain.com/blog/investing-in-cybersecurity-are-you-overspending-or-underspending>
28. Harvard Business Review. (2018). *Why Compliance Programs Fail—and How to Fix Them*. Retrieved from <https://hbr.org/2018/03/why-compliance-programs-fail>.

Glossary

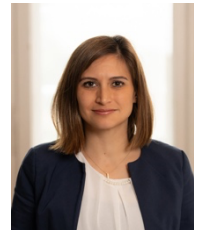
Abbreviation	Description
BSI	German Federal Office for Information Security
CCPA	California Consumer Privacy Act
CRA	Cyber Resilience Act
DACH	Germany, Austria, and Switzerland
DORA	Digital Operational Resilience Act
GDPR	General Data Protection Regulation
GenAI	Generative Artificial Intelligence
ISMS	Information Security Management Systems
ISO	International Organisation for Standardisation
KYC	Know Your Customer
LoD	Line of Defense

Authors

Leon Kuhlmann is Managing Director at Grey Swan and has almost 10 years of experience in management and IT consulting. He has managed and implemented complex and extensive (IT) transformation programs in various industries and regions, including (IT) audits, with an understanding of compliance. His core competencies include program and turnaround management.



Nadine Hofmann is a Director at Grey Swan. She is a compliance expert for information security management systems (ISMS) and data protection information management systems (PIMS) according to ISO 27001. Her experience includes implementing measures for financial institutions by designing processes and mitigating bank audit findings.



Farahnoz Mirboboeva is a Manager at Grey Swan. She has extensive experience in consulting, with a focus on the implementation of information security management systems, project management, and strategy development. Her projects include reviewing core banking systems, preparing for audits, remediating audit findings, and developing business and IT strategies.



Victoria Denisiuk is an Associate at Grey Swan. She specialises in digital transformation including strategic modernisation, intelligent automation, and information systems optimisation. With expertise spanning business analysis, project management, and technology delivery, she drives operational efficiency and secure solutions for enterprises.



About Grey Swan

In an era characterised by constantly changing geopolitical and macroeconomic challenges, volatility has become a constant companion. The combination of these diverse challenges has significantly increased the probability of the occurrence of so-called „Grey Swan“ events. These events, often of an unpredictable nature, have a profound impact on investments, organisations, industries, or entire economies.

Our approach to an evolving environment is strategic resilience. We offer expert advice in today’s complex business world with a diverse and carefully developed service portfolio. Our consulting services focus on addressing risk, compliance, and use of technology. This is done through the design of risk management structures, the optimisation of financial functions, the resolution of technological obstacles, and the strict adherence to regulatory and legal compliance standards. We also contribute to the management of complex programs to enable our clients to ensure their „Strategic Resilience“.

Copyright Claim

The contents of this publication are protected by copyright, and any reproduction of this content, in particular the use of texts, parts of texts, entire sections or graphic representations, requires the prior permission of Grey Swan Management AG. The information present-ed is for informational purposes only and may not always be current and is subject to interpretation. Verification of information should be carried out independently. We assume no liability for any errors, omissions or inaccuracies in the content and for the consequences of use of the information, nor are we responsible for any content on third-party websites. The authors reserve the right to change, update or remove the content of the publication as necessary. The logos or trademarks shown in text or graphics belong to their respective companies. Grey Swan Management AG uses them exclusively for educational purposes and does not claim ownership rights to these logos.

Grey Swan Management AG
Baarerstrasse 52
6300 Zug | Switzerland
www.greyswan.ch
Office: +41 43 505 23 22
Contact: ch.office@greyswan.ch

Copyright © Grey Swan Management AG

June 2024

