Grey Swan

New Order

Program Management under New Regulatory Requirements

Leon Kuhlmann

Julius Düwel

Pauline Schmidt

Tamino Müller

Grey Swan Management AG

April 2024

White paper

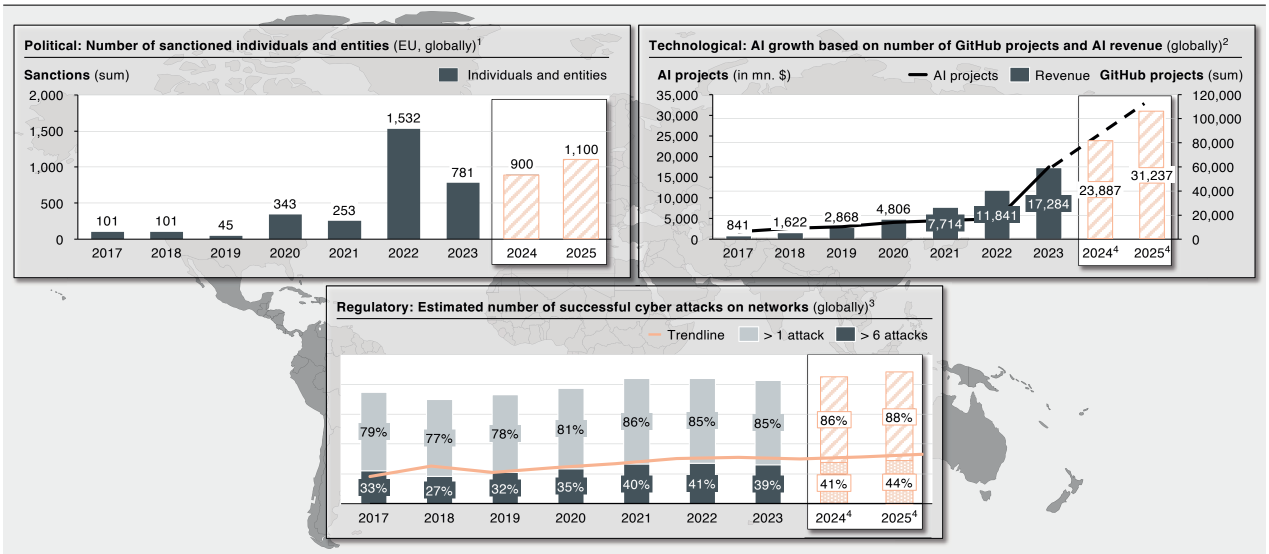
Management Summary

- Businesses face a range of challenges that significantly influence their strategies and the sustainability of their operations in evolving markets, including political, technological, and regulatory factors.
- Regulatory changes in Europe are intensifying the challenges faced by companies and critical infrastructure organisations (CRITIS). These challenges are further compounded by comprehensive and largely sector-agnostic regulatory standards such as the Network Information Security Directive 2.0 (NIS2), the Critical Entities Resilience Directive (CER), the Cyber Resilience Act (CRA), the General Data Protection Regulation (GDPR), and the Digital Operational Resilience Act (DORA).
- Integrating these laws into business operations often poses significant challenges for companies. These include managing cross-market dependencies without regulatory conflicts while operating in multiple countries, navigating political uncertainties, avoiding excessive compliance costs, and coping with the frequent publication of new laws or changes to existing ones and their implementation.
- To ensure positive outcomes from regulatory programs or audits, companies use a framework that includes gap analysis, auditing (with preparation and execution), and remediation involving preparation, planning, and resolution to support operational management.
- Success in these projects depends on three key elements: the availability of methodological expertise, the availability and usage of tools, and the presence of subject matter experts for specialised topics.
- Defect rectification programs in the audit process have unique characteristics. Ideally, they feature robust governance, detailed planning for defect rectification, structured acceptance process for evidences, fact-based reporting, and verification of measures through Test of Design (ToD), Test of Implementation (ToI), and Test of Effectiveness (ToE), culminating in an end-to-end delivery processes.
- The allocation of project management resources for programs, including regulatory programs, can be structured by organisations in three models: insourcing, outsourcing with a RAID approach (Redundant Arrays of Independent Disks, the employment of various service providers to minimise risk), or a hybrid delivery model.

Companies are facing a range of political, technological, and regulatory challenges

Businesses face political, technological, and regulatory challenges due to changing market dynamics. An initial assessment of political challenges shows that penalties for legal breaches, such as GDPR violations, clearly impose significant financial strains on companies. The pace of technological progress demands rapid adoption of emerging technologies like artificial intelligence, which in turn shifts consumer behaviours and alters dynamics within specific business environments. In terms of regulatory issues, the focus shifts to strengthening critical infrastructures, referred to as CRITIS (as outlined in the draft of IT-SiG 3.0, which includes "operators of critical facilities, particularly significant and important facilities"), to protect customer data against the rising frequency of cyber attacks. This goal is pursued by adhering to regulatory standards (Figure 1).

Development and quantification of political, technological, and regulatory challenges



1: Data Europa I 2: GitHub I 3: CyberEdge I 4: Grey Swan Research Institute – Calculation of a forecast based on existing data

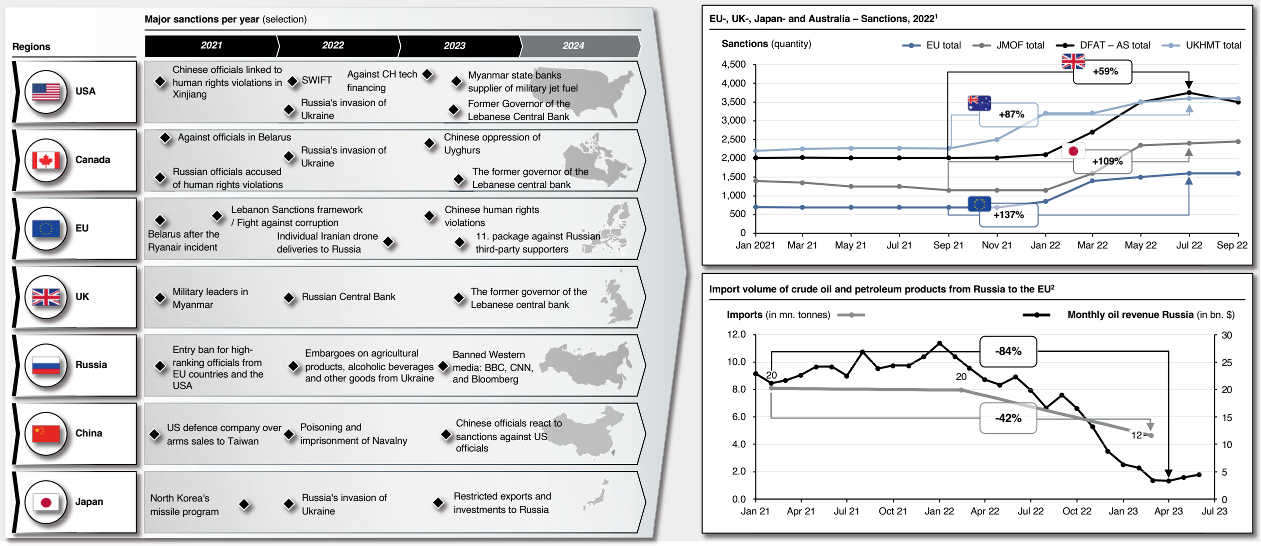
Figure 1: Political, technological, and regulatory challenges

Political challenges emerge when there are violations of laws or business practices that lack political authorisation:

- Firstly, through restrictive measures or "sanctions", which serve as a primary tool of foreign and security policy employed by governments globally. These sanctions target governments of non-EU member states or companies that support the sanctioned policies (Figure 2). They also affect groups or organisations, and individuals under similar conditions[1]. The number of sanctions imposed by the European Union on individuals and entities increased from 101 in 2017 to 1,532 in 2022, marking a rise of 1,417%[2].

- Secondly, regarding supply chain optimisation and management, as mandated by the EU Supply Chain Due Diligence Directive 2022 (CSDDD)3, which requires companies to ensure compliance with legal mandates. Furthermore, it necessitates the evaluation of suppliers for adherence to human rights and environmental standards. This includes influencing the enhancement of sustainability requirements within supply chain management. These requirements significantly exceed existing national legislation, and non-compliance could result in legal repercussions such as civil liability for damages due to omissions, along with substantial fines. The size of which varies based on the severity of the breach.

Overview of the most significant sanctions and consequences of individual actions



Major sanctions per year (selection)

Regions	2021	2022	2023	2024
USA	Chinese officials linked to human rights violations in Xinjiang	SWIFT Russia's invasion of Ukraine	Against CH tech financing Myanmar state banks supplier of military jet fuel Former Governor of the Lebanese Central Bank	
Canada	Against officials in Belarus Russian officials accused of human rights violations	Russia's invasion of Ukraine	Chinese oppression of Uyghurs The former governor of the Lebanese central bank	
EU	Belarus after the Ryanair incident Lebanon Sanctions framework / Fight against corruption	Individual Iranian drone deliveries to Russia	Chinese human rights violations 11. package against Russian third-party supporters	
UK	Military leaders in Myanmar	Russian Central Bank	The former governor of the Lebanese central bank	
Russia	Entry ban for high-ranking officials from EU countries and the USA	Embargoes on agricultural products, alcoholic beverages and other goods from Ukraine	Banned Western media: BBC, CNN, and Bloomberg	
China	US defence company over arms sales to Taiwan	Poisoning and imprisonment of Navalny	Chinese officials react to sanctions against US officials	
Japan	North Korea's missile program	Russia's invasion of Ukraine	Restricted exports and investments to Russia	

Source: Grey Swan Research Institute | 1: Statista, Refinitiv | 2: Federal Statistical Office Germany

Figure 2: Sanction developments, incidents, and consequences

- A third aspect that companies must consider from a regulatory and security policy perspective involves the use of American and Chinese technology stacks. For example, in the telecommunications infrastructure (5G) or in the IT architectures (cloud) of banks and insurance companies, and beyond. Compliance with national regulations for using foreign technologies in critical infrastructures is essential. Notable is the Chinese network provider Huawei. Considered a "high-risk provider" by the European Union, they are now facing exclusion from Germany's 5G infrastructure. Conversely, U.S. technology providers have been delisted in BRICS countries due to more competitive pricing for identical or superior functionality and because of sanctions. This has resulted in an increase in the spread of Chinese technologies in BRICS countries (refer to the white paper "The Dark Knight Rises", Grey Swan 2024).

Therefore, digital competitiveness and the successful adaptation of established technologies are crucial for success.

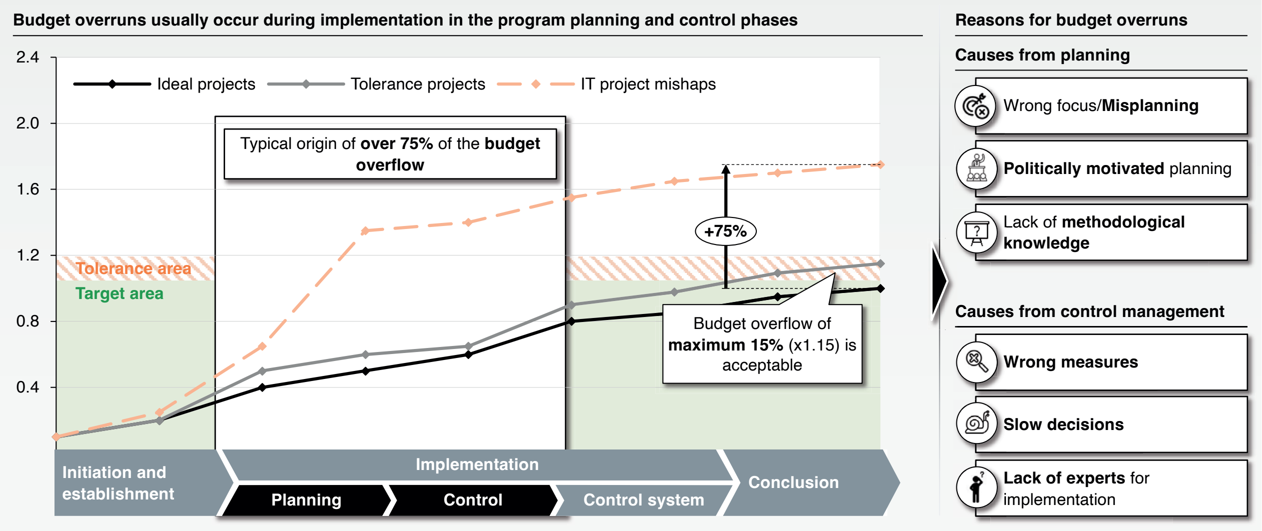
- The widespread use of artificial intelligence as a personalised tool, such as in customer communications through chatbots, voice support, or assistance, is setting the stage. In production, data is also collected on an event-driven basis and analysed largely automatically[4].

- Moreover, the use of cloud computing has now become common amongst major companies. The primary cloud modules employed are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Gartner's prediction that 70% of companies will be using enterprise cloud solutions by 2027 suggests that cloud computing is not merely a trend but a strategic business decision[5].

- Additional challenges encompass front-end developments such as "low code/no code" platforms. For instance, using "drag-and-drop" tools, which are anticipated to constitute more than 80% of software development occurring outside IT departments[6]. "Chatbots and AI" are being used to generate code through intelligent code suggestions for data analysis and testing, as well as "microservice architectures" that employ separate code bases to enhance scalability and modularity. Additionally, "voice-activated technology" is utilised for controlling smart homes, mobile phones, and car systems. All these technologies are increasingly becoming integrated into everyday business and IT operations.

Regulatory challenges are pervasive across all industries, with companies operating in critical infrastructure sectors being particularly impacted. This is a by-product of the introduction and evolution of existing regulations, which are accompanied by numerous requirements that must be met.

Development of budget costs for large-scale IT projects



Source: University of Oxford

Figure 3: Development of costs for large-scale IT projects

- On the one hand, there are financial regulations mandated nationally by banking regulatory authorities and central banks, monitored for compliance. Examples include the Basel III reforms (also known as Basel IV)[7] and MaRisk (minimum requirements for risk management)[8].

- On the other hand, cyber security regulation in Europe is covered by the NIS2 along with its physical counterpart the CER, and the Cyber Resilience Act (CRA)[9], the “General Data Protection Regulation” (GDPR)[10], and the Digital Operational Resilience Act (DORA)[11], with corresponding national laws outside the EU. For further insights and detailed information on these regulations, refer to the white paper “King of the Audits”, Grey Swan 2024.

- The regulation of Environmental, Social, and Governance (ESG) factors is also gaining importance through stricter laws and harsher consequences. An example is the ESG EU Corporate Sustainability Reporting Directive (CSRD)[12], which mandates companies to engage in non-financial reporting. Additionally, initiatives like the United Nations Sustainable Development Goals (SDGs)[13] and frameworks such as the Global Reporting Initiative (GRI)[14] promote actions within the ESG domain.

The USD 25 million fine imposed on DWS by the US Securities and Exchange Commission (SEC) in September 2023 for non-compliance with regulatory requirements is an example of the increased global regulatory measures. Firstly, DWS was criticised for having an inadequate anti-money laundering program for its investment funds, with a lack of implementation of required guidelines and inadequate management training. Secondly, DWS published false information about its investment process, with key aspects not effectively implemented between 2018 and 2021, resulting in misleading information about ESG practices[15]. Crédit Agricole was likewise fined 1.5 million EUR by the French financial supervisory authority in 2022 for deficiencies in transaction monitoring and customer due diligence[16]. These challenges require management through projects with a defined scope, timeline, and budget. This requires methodological expertise, tool support, and access to expert knowledge. Examples of this are IT audits (e.g., Solarisbank[17], N26[18]), digitalisation projects such as modernising the IT landscape through new software implementations (e.g., DB-Postbank[19], Deutsche Bahn[20]), integration of AI platforms (e.g. Vodafone[21], Siemens[22]), and mergers & acquisitions transactions (e.g., ROHM Co. Ltd[23], Microsoft[24]). These projects are integral to strategic corporate objectives, impact various company divisions, and are characterised by their complexity.

Regulatory requirements continue to increase horizontally (more supervised companies) and vertically (more detailed requirements)

Effective program management, which involves coordinating multiple projects, is crucial for the success of such initiatives. Without effective program management, there is a significant risk of projects experiencing overruns in scope, time, and budget (Figure 3).

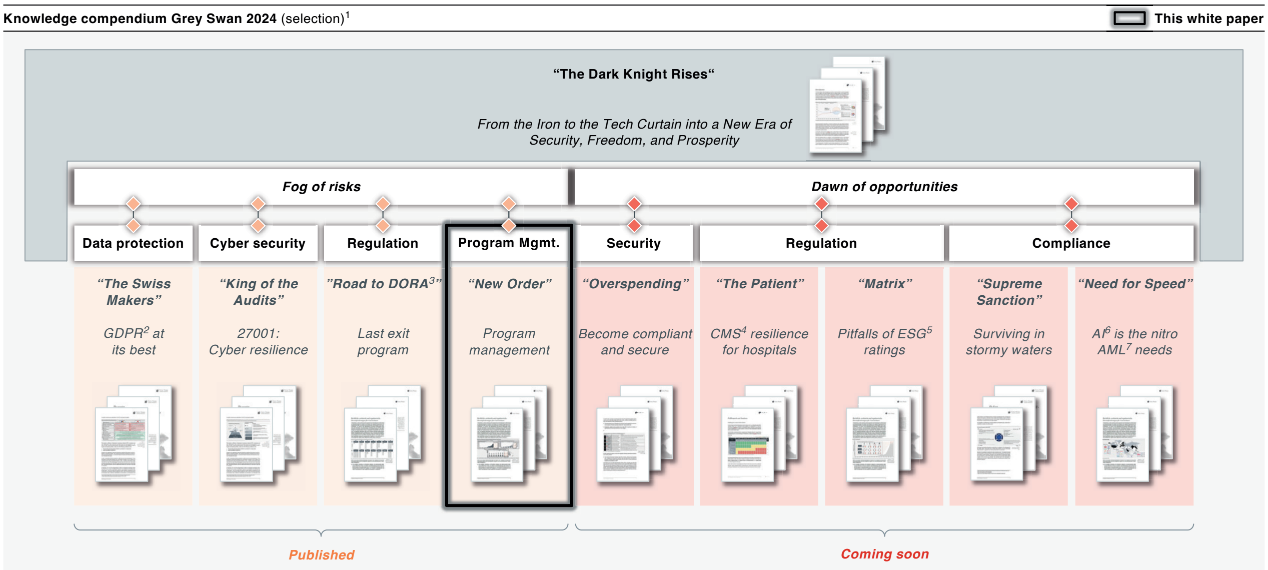
In the following, we examine the experience of designing and managing highly complex programs using the example of an IT audit.

All industries that are categorised as critical infrastructure, such as telecommunications, energy, finance, and healthcare, must have IT audits conducted.

Financial institutions which are currently subject to national regulations under the umbrella of the European supervisory authorities (EBA[25]), European Insurance and Occupational Pensions Authority (EIOPA[26]) and the European Securities and Markets Authority (ESMA[27]) as well as the respective national supervisory authorities, from the beginning of 2025 under the DORA, must pass IT audits.

This paper contributes to a comprehensive knowledge compendium, encompassing expertise in data protection, cyber security, and regulatory frameworks, among other areas (Figure 4).

The paper examines regulatory developments within the financial markets concerning IT audits. Followed by an exploration of the challenges in adhering to regulatory requirements by the supervised entities. We will then present example solutions for managing an audit, and conclude with a discussion on how to effectively establish a successful project management framework within an organisation.



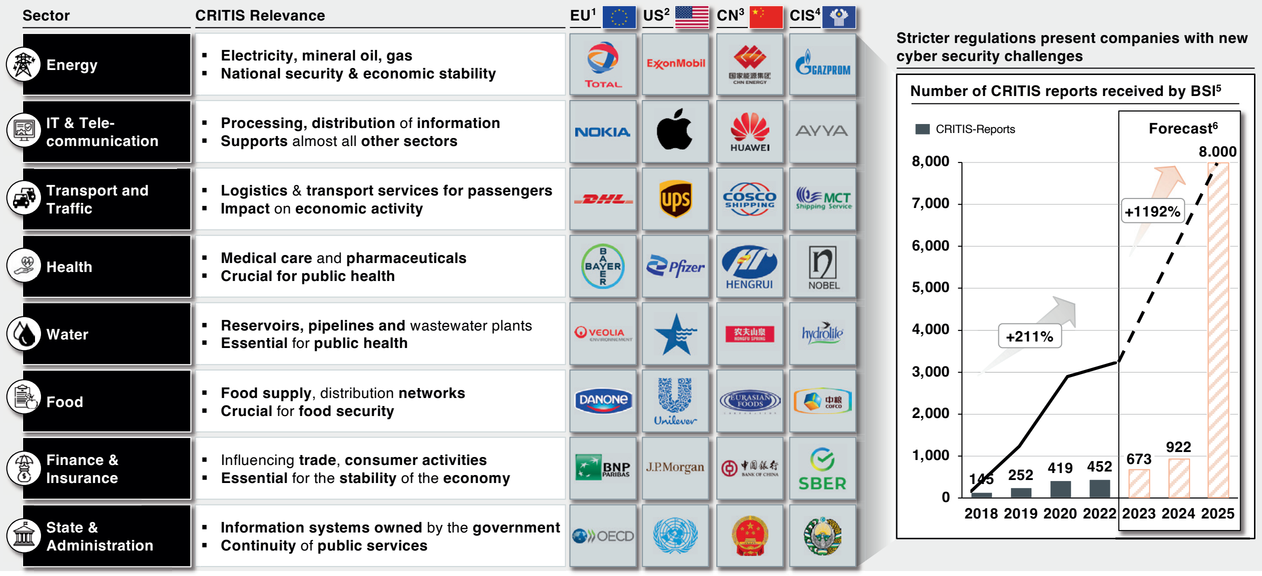
Source: Grey Swan I 1: Further publications available on request I 2: GDPR = General Data Protection Regulation I 3: DORA = Digital Operational Resilience Act I 4: CMS = Compliance Management System I 5: ESG = Environmental, Sustainability, Governance I 6: AI = Artificial Intelligence I 7: AML = Anti-Money Laundering

Figure 4: Overview of competence areas

Regulatory developments increase regulatory challenges

The significance of critical infrastructures (CRITIS) for the national community and their classification across various sectors such as energy, IT and telecommunications, transport and traffic, health, water, food, finance and insurance, municipal waste disposal as well as government and administration is evident[28]. These sectors are essential due to their central role in the functioning of the community and the risks associated with failures or disruptions. This requires active CRITIS notifications to the regulator (Figure 5). The average cost of data breaches due to regulatory non-compliance in these industries is USD 5.04 million, which is 28.6% higher on average than in other sectors. This highlights the importance of compliance and risk management in CRITIS companies.

Data and cyber security in 8 critical infrastructure sectors (CRITIS) is essential for economic activity, public health and national security



Sector	CRITIS Relevance	EU[1]	US[2]	CN[3]	CIS[4]
Energy	▪ **Electricity, mineral oil, gas** ▪ **National security & economic stability**	TOTAL	ExxonMobil	国家能源集团 CHN ENERGY	GAZPROM
IT & Tele-communication	▪ **Processing, distribution** of **information** ▪ **Supports** almost all **other sectors**	NOKIA		HUAWEI	AYYA
Transport and Traffic	▪ **Logistics** & **transport services for passengers** ▪ **Impact** on **economic activity**	DHL	ups	COSCO SHIPPING	MCT Shipping Service
Health	▪ **Medical care** and **pharmaceuticals** ▪ **Crucial for public health**	BAYER	Pfizer	HENGRUI	NOBEL
Water	▪ **Reservoirs, pipelines and** wastewater plants ▪ **Essential** for **public health**	VEOLIA ENVIRONNEMENT		农夫山泉 NONGFU SPRING	hydrolife
Food	▪ **Food supply**, distribution **networks** ▪ **Crucial** for **food security**	DANONE	Unilever	EURASIAN FOODS	中粮 COFCO
Finance & Insurance	▪ Influencing **trade, consumer activities** ▪ **Essential** for the **stability** of the **economy**	BNP PARIBAS	J.P.Morgan	中国银行 BANK OF CHINA	SBER
State & Administration	▪ **Information systems owned** by the **government** ▪ **Continuity** of **public services**	OECD			

Stricter regulations present companies with new cyber security challenges

Number of CRITIS reports received by BSI[5]

1: EU = European Union I 2: US = United States I 3: CN = China I 4: CIS = Commonwealth of Independent States I 5: BSI = German Federal Office for Information Security I 6: Grey Swan Research Institute 3-year forecast based on 2 push factors (effects from digitalisation and increase in affected companies to approx. 30,000 through NIS 2 entry into force) and 1 pull factor (effects from implementation of new laws)

Figure 5: 8 CRITIS sectors for national economic viability and security

This raises the question of how the regulatory framework for CRITIS companies is developing and changing to ensure their ability to function.

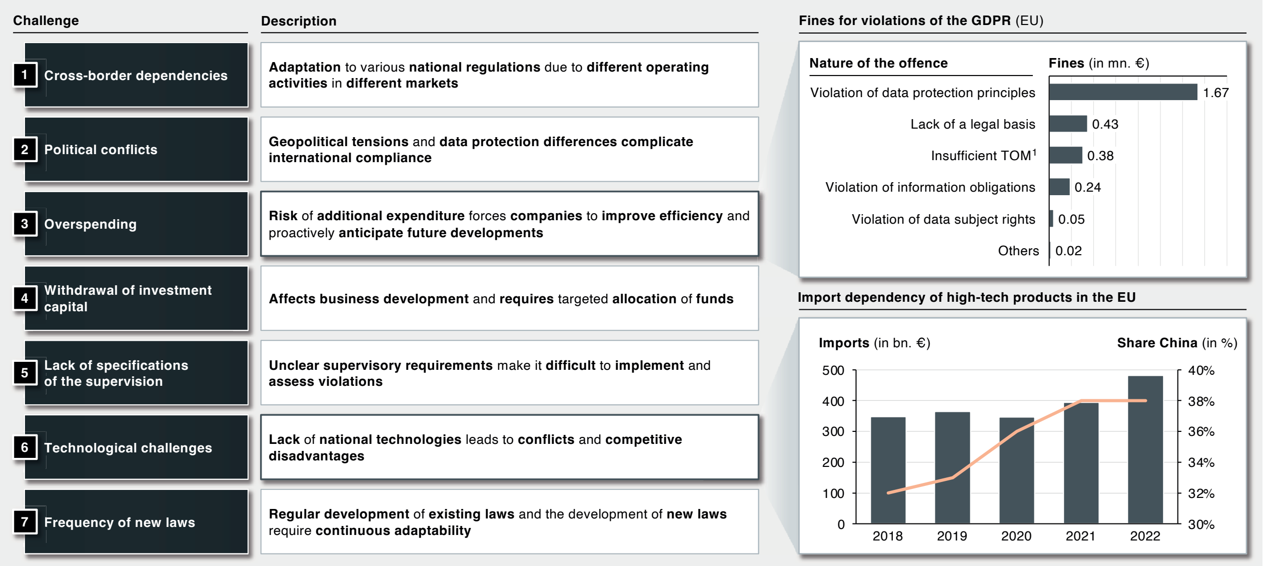
By 2025, almost all relevant and overarching CRITIS laws in Europe and Switzerland will be updated or newly introduced (Figure 5). Compared to the NIS1 version[29], the Network Information Security Directive version 2.0 (NIS2)[30] extends cyber security requirements to encompass more sectors and more companies.

The principle of lex specialis applies particularly to the financial sector, specifying the conditions under which both DORA and the NIS2 set out requirements. If DORA's stipulations are more specific, they override those of the NIS2. The final regulations are governed by the NIS2 Implementation Act. In our white paper titled King of the Audits", Grey Swan 2024 we thoroughly explore these regulatory developments and provide clear solutions for integrating all legislative mandates within a framework.

7 challenges for companies in implementing regulatory requirements

Compliance, traditionally viewed as a cost centre similar to cyber security and data protection, involves tasks that are frequently seen as imposed and not intended to disrupt operations. Efforts are made to minimise internal and external costs as much as possible. As long as there are no incidents, everything is considered “fine”. At best, the value of compliance is recognised through the avoidance of penalties such as fines, restrictions on growth for acquiring new customers over a period, or limits on the maximum loan amounts that can be issued. The outcomes of this approach are evident in non-monetary, monetary, and legal consequences.

Challenges in the processing of regulatory requirements by the supervisory object



Challenge	Description
1 Cross-border dependencies	**Adaptation** to various **national regulations** due to **different operating activities** in **different markets**
2 Political conflicts	**Geopolitical tensions** and **data protection differences complicate international compliance**
3 Overspending	**Risk** of **additional expenditure** forces **companies** to **improve efficiency** and proactively **anticipate future developments**
4 Withdrawal of investment capital	**Affects business development** and **requires** targeted **allocation** of **funds**
5 Lack of specifications of the supervision	**Unclear supervisory requirements** make it **difficult** to **implement** and **assess violations**
6 Technological challenges	**Lack** of **national technologies** leads to **conflicts** and **competitive disadvantages**
7 Frequency of new laws	**Regular development** of **existing laws** and the development of **new laws** require **continuous adaptability**

Fines for violations of the GDPR (EU)

Nature of the offence	Fines (in mn. €)
Violation of data protection principles	1.67
Lack of a legal basis	0.43
Insufficient TOM[1]	0.38
Violation of information obligations	0.24
Violation of data subject rights	0.05
Others	0.02

Import dependency of high-tech products in the EU

Source: Grey Swan I 1: Technical and organisational measures

Figure 6: The challenges posed by regulatory requirements are multifaceted

Therefore, compliance extends beyond current topics such as ChatGPT or AI; it offers far more than simply adherence of legal and self-imposed regulations. The remaining conflict between “production through IT” and “compliance of IT” will remain a key issue in the following years, despite complete digitalisation. DORA will become fully enforceable from January 2025.

With additional European security regulations such as NIS2 and CER, a surge in requirements similar to the introduction of the GDPR can be anticipated. Furthermore, internal conflicts may escalate due to varying interpretations of technology in implementing risk management into work culture. But also due to differing assessments of operational risk management options through inherently resilient system architectures. Challenges in the processing of regulatory requirements by the supervisory object can therefore vary (Figure 6).

1. A commonality amongst CRITIS companies is multiple market operation. They are exposed to several national regulatory realities (cross-market dependency). This increased complexity poses a substantial challenge for compliance departments as well as management.

2. The current geopolitical environment reveals political uncertainties as relevant barriers to the implementation of regulatory requirements. Therefore, de-risking is required. The procurement of raw materials, utilisation of technologies, and management of knowledge are subject to increasingly stringent regulations. Meanwhile, Europe, the USA, and China have contrasting approaches to data protection. The transfer of expertise has always been subject to political interests. These uncertainties must also be considered when realising projects with international partners, or service providers.

3. Financial management frequently encounters the issue of "overspending" on compliance requirements, as non-compliance with a legal requirement is associated with severe sanctions and subsequent correction with high additional costs. Therefore, it is presented with the challenge of enhancing efficiency of compliance with regulatory developments and anticipating future developments at low cost. A solution to avoid overspending in the area of compliance and information security is explained in the white paper "Overspending", Grey Swan 2024.

4. Overspending goes hand in hand with the withdrawal of investment capital, so that future investments in business development are lower than if the available funds were allocated precisely.

5. Another challenge is the lack of guidelines from the supervisory authority. Neither the implementation of requirements nor the interpretation of the severity of a potential finding are defined. Regarding the Supply Chain Due Diligence Act (SCDDA), 63% of organisations feel that they are "moderately to very poorly" prepared[31].

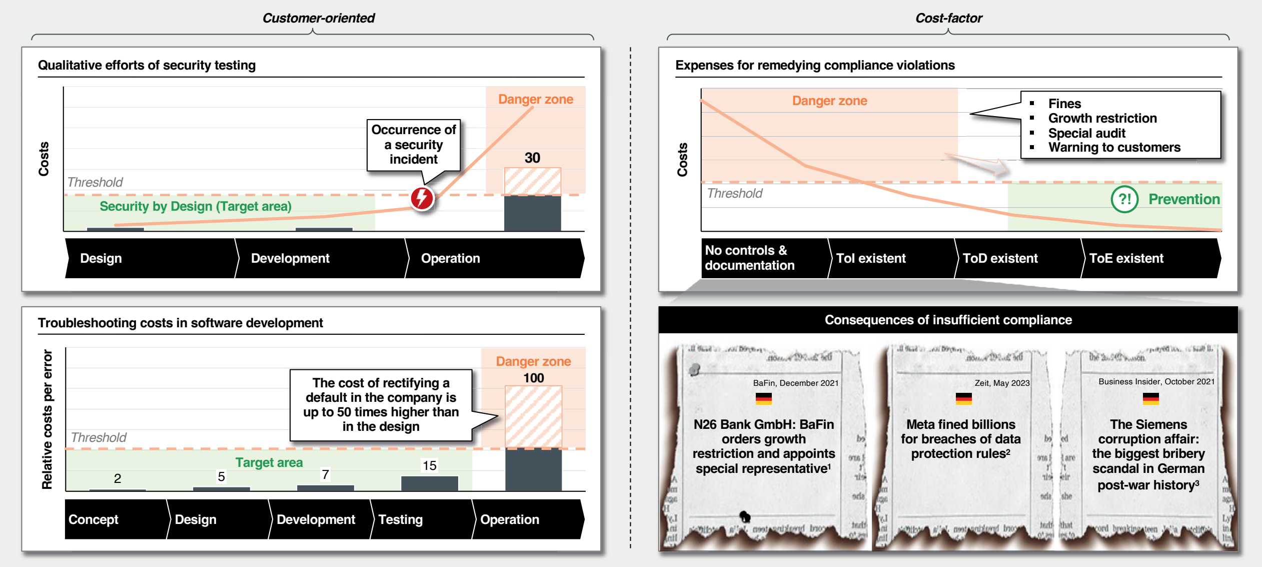
6. The implementation poses a challenge for affected companies due to the technological realities of their installed base. Due to the unavailability of national infrastructure technologies, whose use is imperative for enforcing efficiency advantages, there is a need to rely on international technologies. This can lead to conflicts with regulators or even to competitive disadvantages. International technology providers are often reluctant and cautious in implementing the requirements of national regulators. Additionally, ensuring a cyber-resilient supply chain, in which companies must check their own supply chains as well as those of their suppliers, presents a problem.

Increasingly complex regulatory requirements raise the importance of project and program management

7. The frequency of legislation publication, as well as the updating and changing of requirements in existing frameworks, requires a continuous review process to determine whether and which regulatory requirements are in force or imminent. This allows for their procedural, organisational, and technical implementation. For instance, under NIS2, the basis of assessment for critical infrastructure (CRITIS) companies was changed from the products produced, such as the amount of treated drinking water per year, to a fixed classification: Eleven sectors are classified as high criticality and seven with other criticalities. Which facilities are considered "essential" and which are "important" is thus determined by their belonging to a particular sector and their size, measured by revenue and the number of employees.

Figure 7 demonstrates the consequences of not considering the previously mentioned seven points. It becomes evident that companies in critical infrastructure sectors, as well as in adjacent sectors, need to monitor regulatory developments, regularly verify their compliance, and ensure implementation.

Development of the distribution of compliance costs in the life cycle is similar to that of software development and security testing



Customer-oriented
Cost-factor
Qualitative efforts of security testing
Costs
Danger zone
Occurrence of a security incident
30
Threshold
Security by Design (Target area)
Design
Development
Operation
Troubleshooting costs in software development
Relative costs per error
Danger zone
100
The cost of rectifying a default in the company is up to 50 times higher than in the design
Threshold
Target area
2
5
7
15
Concept
Design
Development
Testing
Operation
Expenses for remedying compliance violations
Costs
Danger zone
Fines
Growth restriction
Special audit
Warning to customers
Threshold
?!
Prevention
No controls & documentation
ToI existent
ToD existent
ToE existent
Consequences of insufficient compliance
BaFin, December 2021
N26 Bank GmbH: BaFin orders growth restriction and appoints special representative¹
Zeit, May 2023
Meta fined billions for breaches of data protection rules²
Business Insider, October 2021
The Siemens corruption affair: the biggest bribery scandal in German post-war history³

Source: Grey Swan Research Institute I 1: BaFin I 2: Zeit I 3: Business Insider

Figure 7: Equal distribution of troubleshooting costs in the life cycle of essential processes

The Grey Swan Audit Framework for overcoming challenges

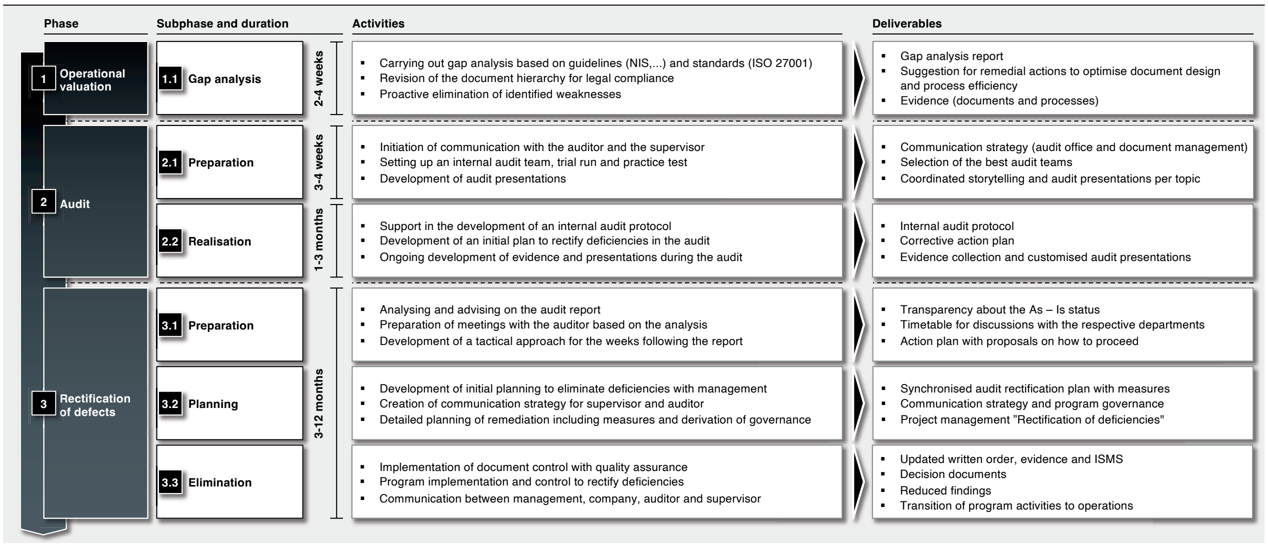
For audit situations in critical infrastructure, it is fundamental to establish a binding framework for the entire process, from the announcement of the audit to the rectification of defects.

It is suitable to use a framework that serves as a guide and consistently distinguishes between audit phases with cross-phase activities. Depending on the phase, different activities and outcomes are in focus, which are ensured through a tailored approach. Although the application of a framework, especially in more complex audit situations where audit preparation and execution require the establishment of a resilient and professional defence line, and defect rectification can only be managed as a program, plays a critical role, the use of a framework is generally advisable.

This way, the best possible results in the audit and for the audit report can be achieved, to exert the greatest possible influence on the regularly high efforts before the defect rectification. The Grey Swan Audit Framework brings together diverse experiences from CRITIS protection, compliance, Information Security Management Systems (ISMS), and program management in a comprehensive and proven framework (Figure 8).

The framework integrates methods and tools designed for audit situations, which are coordinated with each other. This allows for a structured approach to be enforced and the completeness of the audit management to be guaranteed. It enables the management of critical points (for example, the delta report from the gap analysis, interviews in the audit preparation and execution, collaboration with auditors, reports to the national supervisory authority, or the plan for defect remediation).

The Grey Swan Audit Framework generally comprises 3 phases with a total of 6 sub phases and corresponding results



Phase	Subphase and duration		Activities	Deliverables
1 Operational valuation	1.1 Gap analysis	2-4 weeks	▪ Carrying out gap analysis based on guidelines (NIS,...) and standards (ISO 27001) ▪ Revision of the document hierarchy for legal compliance ▪ Proactive elimination of identified weaknesses	▪ Gap analysis report ▪ Suggestion for remedial actions to optimise document design and process efficiency ▪ Evidence (documents and processes)
2 Audit	2.1 Preparation	3-4 weeks	▪ Initiation of communication with the auditor and the supervisor ▪ Setting up an internal audit team, trial run and practice test ▪ Development of audit presentations	▪ Communication strategy (audit office and document management) ▪ Selection of the best audit teams ▪ Coordinated storytelling and audit presentations per topic
	2.2 Realisation	1-3 months	▪ Support in the development of an internal audit protocol ▪ Development of an initial plan to rectify deficiencies in the audit ▪ Ongoing development of evidence and presentations during the audit	▪ Internal audit protocol ▪ Corrective action plan ▪ Evidence collection and customised audit presentations
3 Rectification of defects	3.1 Preparation	3-12 months	▪ Analysing and advising on the audit report ▪ Preparation of meetings with the auditor based on the analysis ▪ Development of a tactical approach for the weeks following the report	▪ Transparency about the As – Is status ▪ Timetable for discussions with the respective departments ▪ Action plan with proposals on how to proceed
	3.2 Planning		▪ Development of initial planning to eliminate deficiencies with management ▪ Creation of communication strategy for supervisor and auditor ▪ Detailed planning of remediation including measures and derivation of governance	▪ Synchronised audit rectification plan with measures ▪ Communication strategy and program governance ▪ Project management ”Rectification of deficiencies"
	3.3 Elimination		▪ Implementation of document control with quality assurance ▪ Program implementation and control to rectify deficiencies ▪ Communication between management, company, auditor and supervisor	▪ Updated written order, evidence and ISMS ▪ Decision documents ▪ Reduced findings ▪ Transition of program activities to operations

Source: Grey Swan

Figure 8: The Grey Swan Audit Framework

An in-depth exploration of the audit framework through practical examples and its application in practice is discussed by our Grey Swan compliance experts in the dedicated blog post “Facts and Fiction”, Grey Swan 2024.

Effective program management is critical to the success of the rectification of defects

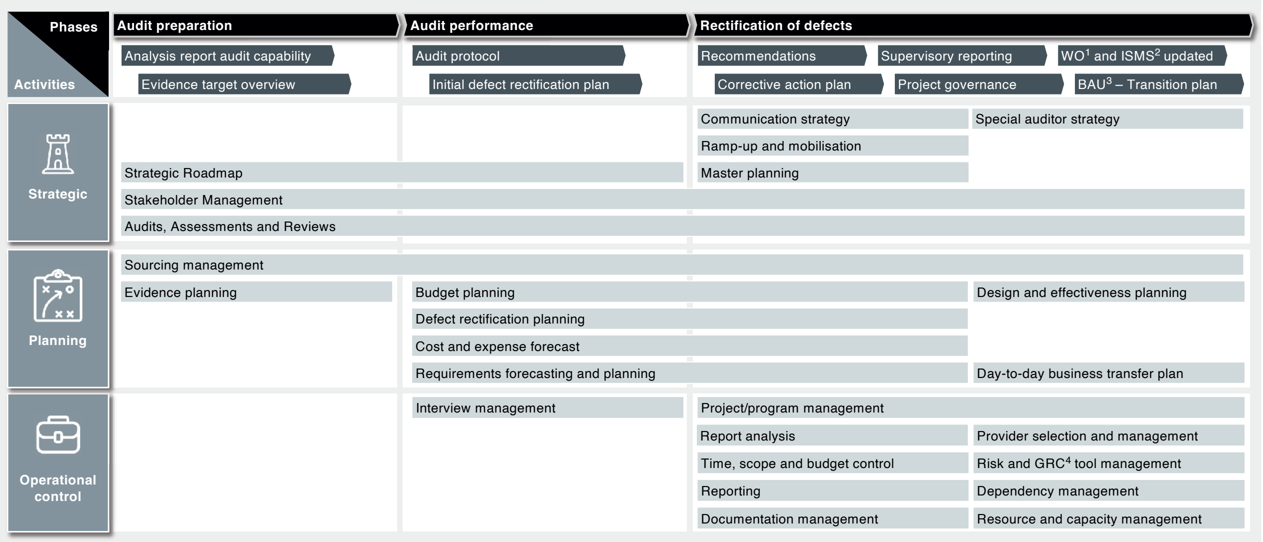
Implementation of a project or program requires methodological competence, tool support, and experts.

Continuing the concept of the audit framework and resolving it through effective program management leads to the development of a ‘Program Audit Framework’ that integrates auditing phases with program management disciplines. (Figure 9).

It connects the phases of “operational assessment”, “audit” (including preparation and implementation support), and “defect rectification” on the timeline with strategic, operational, planning, and control activities on the activities’ axis with the respective relevant contents.

Both axes together constitute a matrix that ensures the controllability of complex projects in the three phases through evidence-based scope definitions.

Phases and activities in audit management



Phases / Activities	Audit preparation	Audit performance	Rectification of defects	
	Analysis report audit capability Evidence target overview	Audit protocol Initial defect rectification plan	Recommendations Corrective action plan Supervisory reporting Project governance	WO[1] and ISMS[2] updated BAU[3] – Transition plan
Strategic			Communication strategy	Special auditor strategy
			Ramp-up and mobilisation	
	Strategic Roadmap		Master planning	
	Stakeholder Management			
	Audits, Assessments and Reviews			
Planning	Sourcing management			
	Evidence planning	Budget planning		Design and effectiveness planning
		Defect rectification planning		
		Cost and expense forecast		
		Requirements forecasting and planning		Day-to-day business transfer plan
Operational control		Interview management	Project/program management	
			Report analysis	Provider selection and management
			Time, scope and budget control	Risk and GRC[4] tool management
			Reporting	Dependency management
			Documentation management	Resource and capacity management

Source: Grey Swan | 1: WO = Written order | 2: ISMS = Information security management system | 3: BAU = Business-as-Usual | 4: GRC = Governance, Risk and Compliance

Figure 9: Phases and activities in audit and program management

Methodological knowledge

Within project management methodology, one must distinguishing between projects and programs. This differentiation is based on factors such as the nature of the goal (operational vs strategic), the timeframe (2-3 months vs. 1-3 years), budget and resource constraints (fixed total budget vs. periodic budget), or criticality for the company (limited vs. company-critical).

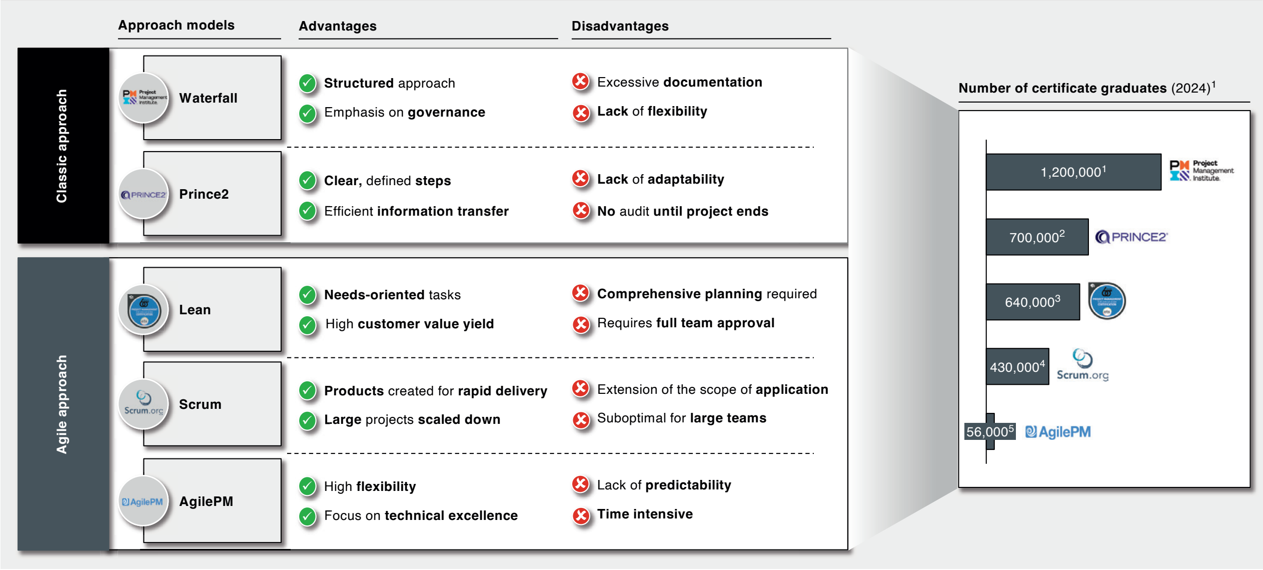
After this decision, the appropriate methodological approach must be chosen, and it must first be clarified whether it is an initiative with a large number of software development activities. If this is the case, agile methodologies such as Lean, AgilePM, and Scrum.org should be used. For other types of initiatives without significant IT efforts, a classic approach following Waterfall or Prince2 may be more appropriate (Figure 10).

In general, programs should follow a lifecycle that includes the phases of initiation and setup, execution (including planning, control, and management), and closure. Moreover, for larger programs, a hybrid approach is often more appropriate, e.g., some projects are managed agilely, others classically following Waterfall, and at the top program level, for example, planning and reporting are done classically.

Methodological knowledge is also required for the disciplines underlying the phases. For example, the initiation phase of a program includes defining the program objectives, setting up the committee structure, or defining roles and responsibilities.

Execution includes mastery of result, resource, cost, dependency, and program planning, as well as control with reporting, risk, outcome and dependency management, and program management, action derivation, and escalation management. At closure, follow-up activities are defined, the final report is created, and the project is handed over.

Comparison of different project management approaches



	Approach models	Advantages	Disadvantages
Classic approach	Waterfall	**Structured** approach Emphasis on **governance**	Excessive **documentation** **Lack** of **flexibility**
	Prince2	**Clear,** defined **steps** Efficient **information transfer**	**Lack** of **adaptability** **No audit until project ends**
Agile approach	Lean	**Needs-oriented** tasks High **customer value yield**	**Comprehensive planning** required Requires **full team approval**
	Scrum	**Products** created for **rapid delivery** **Large** projects **scaled down**	Extension of the scope of **application** Suboptimal for **large teams**
	AgilePM	High **flexibility** Focus on **technical excellence**	Lack of **predictability** **Time intensive**

Source: CRM I 1: Project Management Institute I 2: Prince2 International I 3: Project Management Association I 4: Scum.org I 5: AgilePM

Figure 10: Project managers are more frequently certified in classical process models

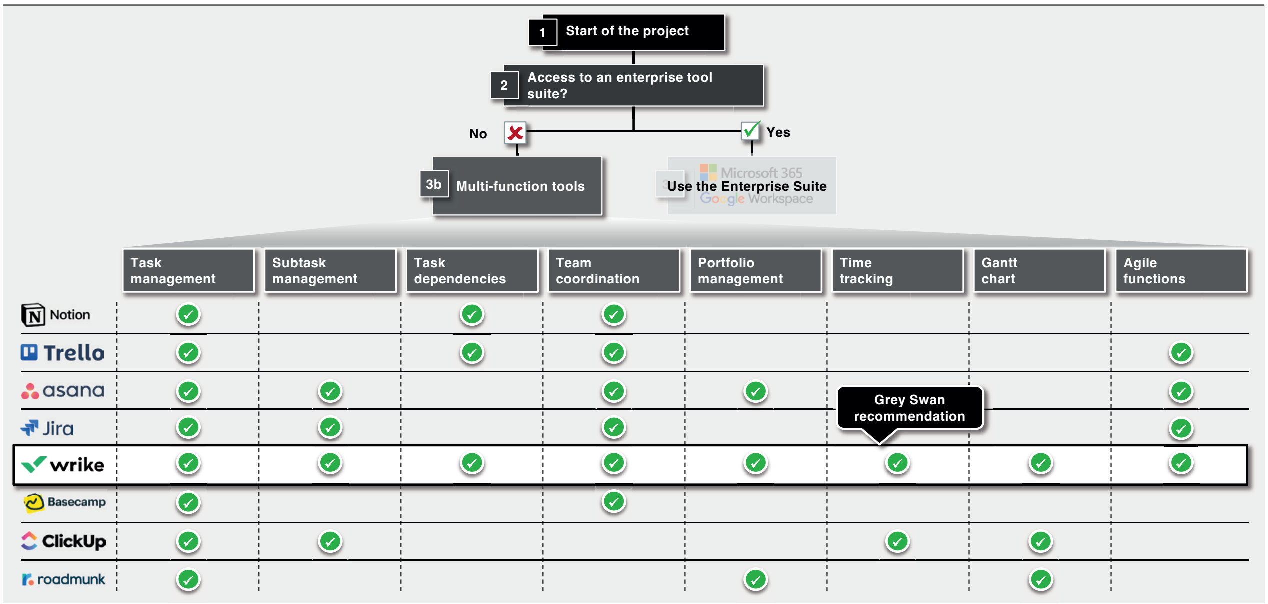
Tool-support

Opting for the correct tools is vital to minimise future administrative efforts, especially in the context of more intricate projects. A report by Dimensional Research Institute indicates that most security experts view the upgrading of their tools (67%) as the primary method for enhancing their company's security posture. However, these efforts are frequently hindered by challenges in integration, a lack of expertise, and the overwhelming number of tools to manage32. When selecting suitable project management tools, it is necessary to consider which software applications are already in use within the organisation, answered by inquiring into the access and availability of an Enterprise Tool Suite (Figure 11).

For example, if working with an Enterprise Suite (e.g., Microsoft 365, Google Workspace, or LibreOffice), the integrated tools within it (e.g., MS Teams and MS Project, G Slides and G Meet, or LibreWriter and LibreImpress) should be utilised. If needed, these can be supplemented with additional tools already integrated into the suite (e.g., Confluence), as employees are already familiar with them. If access to an Enterprise Tool Suite is not available, options include a single-use solution, specialised for a specific requirement, like Trello for task management, or a multi-use solution that covers multiple requirements, like Wrike (our top pick).

The advantage of the correct tool is illustrated by the example of reporting mentioned earlier; only with a uniform, transparent, and fact-based reporting system is it possible to create standard reports for regularly meeting project committees, as well as to accommodate ad-hoc requests and increase efficiency in project management. For reporting, a dedicated tool should be mandated as the sole instrument for tracking and reporting (the “Single/Golden Source”) of selected Key Performance Indicators (KPI)”.

Decision tree for project management tools



	Task management	Subtask management	Task dependencies	Team coordination	Portfolio management	Time tracking	Gantt chart	Agile functions
Notion	✓		✓	✓				
Trello	✓		✓	✓				✓
asana	✓	✓		✓	✓			✓
Jira	✓	✓		✓				✓
wrike	✓	✓	✓	✓	✓	✓	✓	✓
Basecamp	✓			✓				
ClickUp	✓	✓				✓	✓	
roadmunk	✓				✓		✓	

Source: Grey Swan Research Institute

Figure 11:
Wrike is the optimal choice
for a multi-functional tool

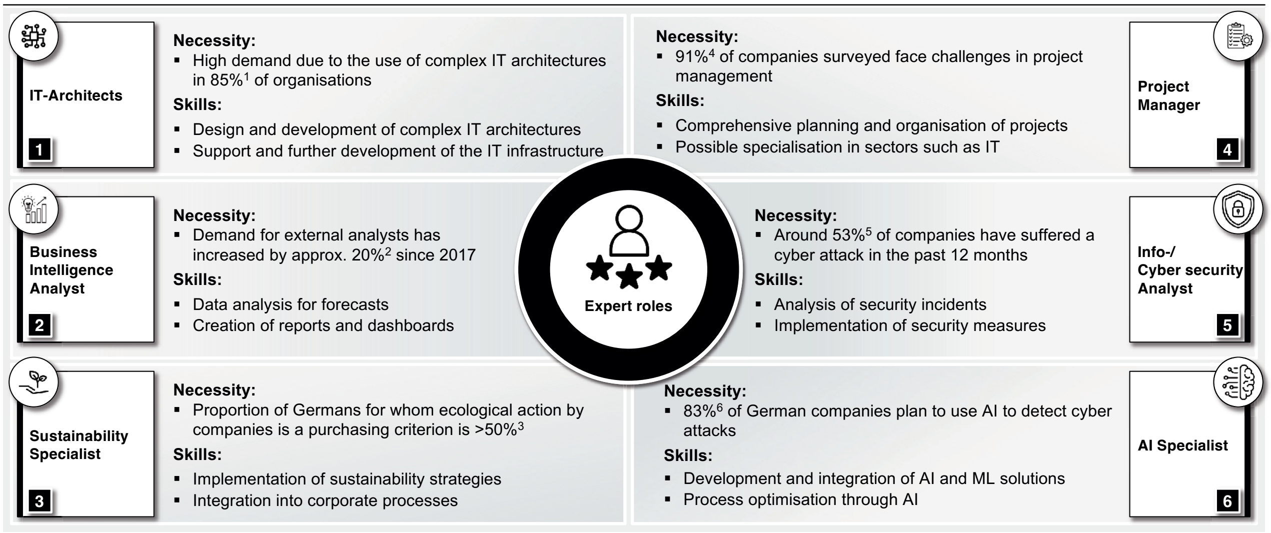
Experts

Experts or subject matter experts (SMEs) are crucial to the success of projects and possess comprehensive knowledge in a specific field of expertise. In times where unlimited internet access might suggest that generalists can replace experts, it is important to recognise that expertise cannot be substituted simply by non-experts who rely on self-research and ad-hoc certifications.

However, this is not the case, especially in complex transformation programs with ambitious timelines or a multitude of involved departments and teams, where competence and experience are of paramount importance. The skills of experts are developed over years, both through practical experiences and through continuous professional training and, education in their field.

To address the identified challenges, especially six experts are needed (Figure 12) to ensure technological innovation, (IT) security, and the processing of regulatory requirements in the modern business landscape.

For example, 91% of surveyed companies face challenges in project management (Project Manager), 85% see a need for experts in the use of complex IT architectures (IT Architect), and 83% plan to deploy AI for detecting cyber attacks (AI specialist). Additional needs exist for information security and cyber security analysts, as well as for sustainability specialists.



Key roles in the modern corporate landscape: IT innovation and security

Expert roles

1 IT-Architects

Necessity:
- High demand due to the use of complex IT architectures in 85%[1] of organisations

Skills:
- Design and development of complex IT architectures
- Support and further development of the IT infrastructure

2 Business Intelligence Analyst

Necessity:
- Demand for external analysts has increased by approx. 20%[2] since 2017

Skills:
- Data analysis for forecasts
- Creation of reports and dashboards

3 Sustainability Specialist

Necessity:
- Proportion of Germans for whom ecological action by companies is a purchasing criterion is >50%[3]

Skills:
- Implementation of sustainability strategies
- Integration into corporate processes

4 Project Manager

Necessity:
- 91%[4] of companies surveyed face challenges in project management

Skills:
- Comprehensive planning and organisation of projects
- Possible specialisation in sectors such as IT

5 Info-/ Cyber security Analyst

Necessity:
- Around 53%[5] of companies have suffered a cyber attack in the past 12 months

Skills:
- Analysis of security incidents
- Implementation of security measures

6 AI Specialist

Necessity:
- 83%[6] of German companies plan to use AI to detect cyber attacks

Skills:
- Development and integration of AI and ML solutions
- Process optimisation through AI

1: Solace I 2: United States Bureau of Labor Statistics I 3: VeMa I 4: Smartsheet I 5: Hiscox I 6: TÜV-Association

Figure 12: Experts in high demand

Solution patterns for implementing a defect rectification program

Crucial success factors for a timely and effective implementation of elimination of defects include:

- ○ Appropriate governance
- ○ Proper communication
- ○ Detailed defect rectification plan
- ○ Structured acceptance process
- ○ Continuous, fact-based reporting
- ○ Verification of measures according to ToD, ToI, and ToE
- ○ Seamless end-to-end result and delivery process

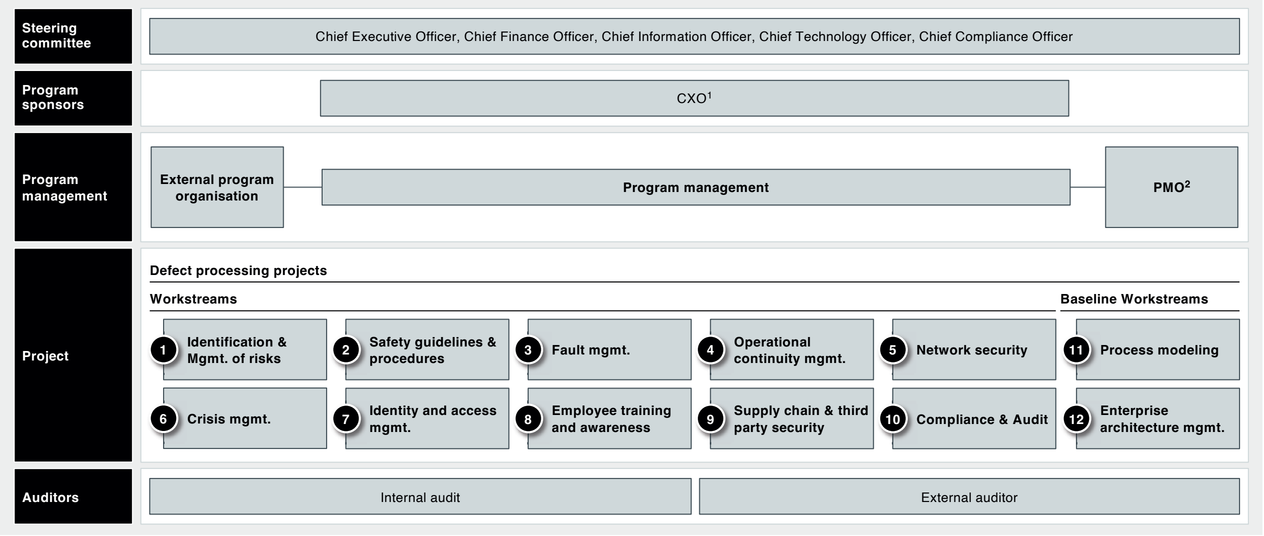
Governance

Ensuring effective defect rectification begins with establishing an appropriate program structure and governance. Clear organisational frameworks should be defined involving pertinent stakeholders, including a steering committee, sponsors, and an empowered program management team tasked with decision-making responsibilities.

This team should comprise program leadership, a Project Management Office (PMO), and the respective rectification projects. External interfaces, such as with the auditor or special representative and the regulatory authority, should be considered. Full participation of the responsible board members in the steering committee is particularly important to ensure optimal control and monitoring of the program. The program leadership coordinates the rectification projects and acts as an interface between executives and special representatives.

To implement these tasks, both an internal and an external Project Management Office can be utilised. To efficiently establish the program structure, the remediation projects should be organised according to the theme groups of the defect rectification plan, so that all deficiencies can be systematically recorded, prioritised, and addressed (Figure 13).

Program structure for rectifying deficiencies in a complex examination situation



Steering committee: Chief Executive Officer, Chief Finance Officer, Chief Information Officer, Chief Technology Officer, Chief Compliance Officer

Program sponsors: CXO[1]

Program management: External program organisation — Program management — PMO[2]

Project: Defect processing projects

Workstreams:

1 Identification & Mgmt. of risks
2 Safety guidelines & procedures
3 Fault mgmt.
4 Operational continuity mgmt.
5 Network security
6 Crisis mgmt.
7 Identity and access mgmt.
8 Employee training and awareness
9 Supply chain & third party security
10 Compliance & Audit

Baseline Workstreams:

11 Process modeling
12 Enterprise architecture mgmt.

Auditors: Internal audit, External auditor

Source: Grey Swan I 1: CXO = C-Level responsible I 2: PMO = Project Management Office

Figure 13: Exemplary program structure and governance

Communication with the supervisory authority and development of a strategy

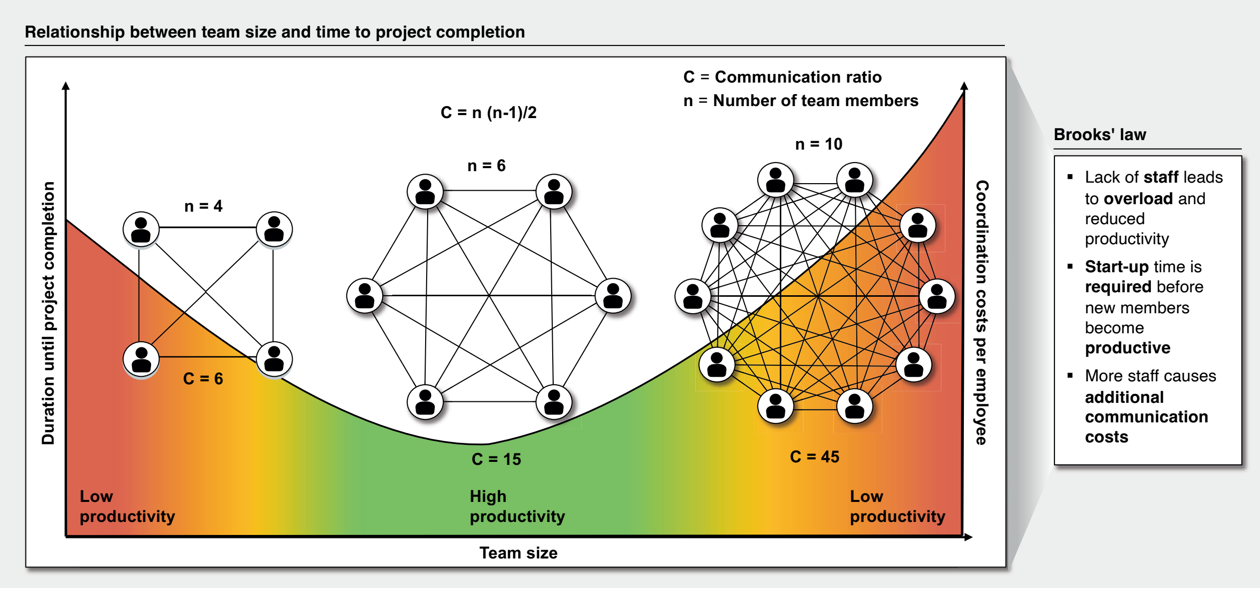
When commencing a deficiencies rectification program, the primary emphasis lies in communicating with the supervisory authority, internal bodies (such as risk management, compliance, and decision-making bodies), and various departments.

Additionally, it is necessary to identify action options, as well as to evaluate and prepare the options for decision-making. The benchmark for this is always the analysis of the audit report. Moreover, ensuring the preparation for upcoming meetings with the supervisory authority, based on the analysis results, as well as the development of a tactical and strategic approach alongside a communication strategy, is essential. Programs are typically company-wide and involve various organisational groups, bodies, and departments.

In developing the communication strategy, similar to establishing the program governance, the high number of internal and external stakeholders inherent in a defect rectification program should be taken into account. This means that auditors (internal audit, external auditor) are involved in various projects for addressing deficiencies with employees from the responsible departments.

Additionally, project organisation committees and decision-makers are involved. Therefore, it is crucial to prevent communication relationships from becoming a paralysing factor (Figure 14) for factual progress.

As the number of team members within a project increases, so does the complexity of communication



Relationship between team size and time to project completion
C = Communication ratio
n = Number of team members
C = n (n-1)/2
n = 4
C = 6
n = 6
C = 15
n = 10
C = 45
Duration until project completion
Coordination costs per employee
Team size
Low productivity
High productivity
Low productivity
Brooks' law
Lack of staff leads to overload and reduced productivity
Start-up time is required before new members become productive
More staff causes additional communication costs

Source: Brooks Jr, F. P.

Figure 14: Illustration of Brooks' law

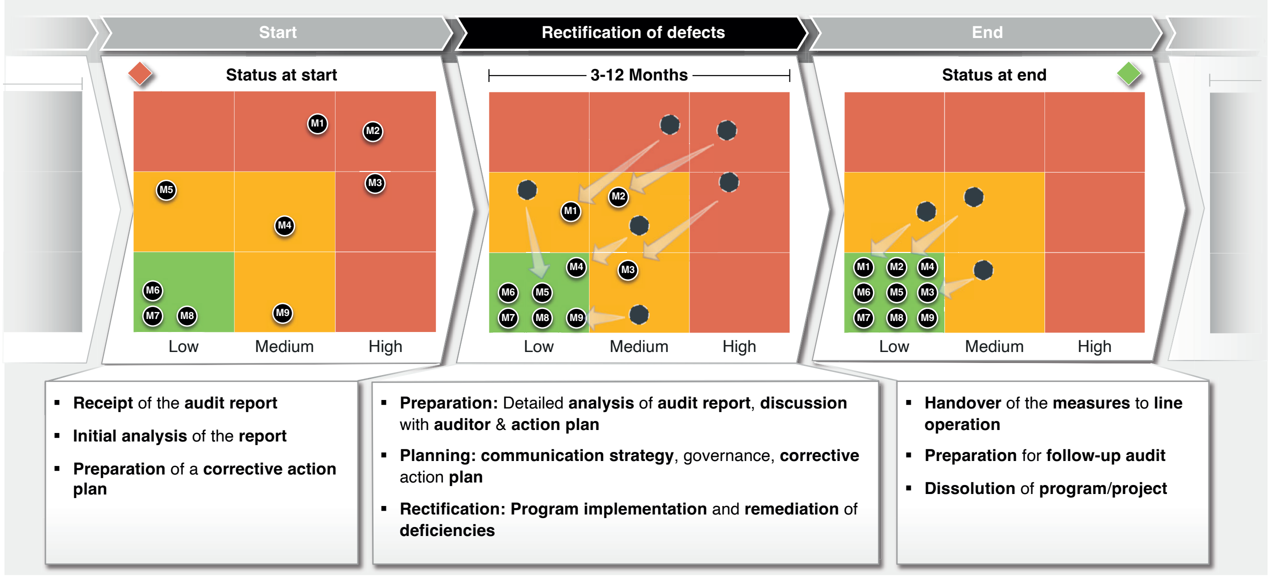
Defect rectification plan

The objective of implementing a defect rectification plan is to ensure that the written order is regularly updated to meet legal compliance requirements, securely document management decisions and approvals for audit purposes, minimise findings, and seamlessly integrate audit program activities into daily business operations. The creation of a defect rectification plan, focusing on reducing deficiencies, is indispensable. For instance, following the model of the framework developed by C. Böhning, who was active at a Berlin technology think tank, as part of a defect rectification program at a German international large bank (Figure 15).

Before beginning the reduction of findings, it is important to classify all findings according to severity (deficiency list with implementation plan following BaFin guidelines), urgency, and feasibility. A careful assessment of the findings is essential to ensure that limited resources are effectively utilised, and a rapid reduction of findings can be achieved.

After an assessment of the findings has been conducted, a swift reduction of the “high/very high” or F3/F4 findings should be focused on to achieve a stable state. The most critical rectification projects should be prioritised and coordinated. During the elimination process, the focus is on securing the results of the already processed “high/very high” findings. In addition, the processing of non-critical findings (“low” and “medium” or F1/F2) is targeted to establish a solid foundation for regular operations. The implemented technical-organisational measures are reviewed for their effectiveness and adjusted if necessary. Once sufficient effectiveness (ToE) has been demonstrated in the form of described (ToD) and implemented (ToI) processes and the non-critical findings have been addressed, the review and conclusion of the defect rectification plan should be initiated.

Schematic representation of the rectification of defects after receipt of the audit report Severity: 🟩 Low 🟨 Medium 🟥 High



- **Receipt** of the **audit report**
- **Initial analysis** of the **report**
- **Preparation** of a **corrective action plan**

- **Preparation:** Detailed **analysis** of **audit report**, **discussion** with **auditor** & **action plan**
- **Planning: communication strategy**, governance, **corrective** action **plan**
- **Rectification: Program implementation** and **remediation** of **deficiencies**

- **Handover** of the **measures** to **line operation**
- **Preparation** for **follow-up audit**
- **Dissolution** of **program/project**

Source: C. Böhning

Figure 15: Prioritising the rectification of defects

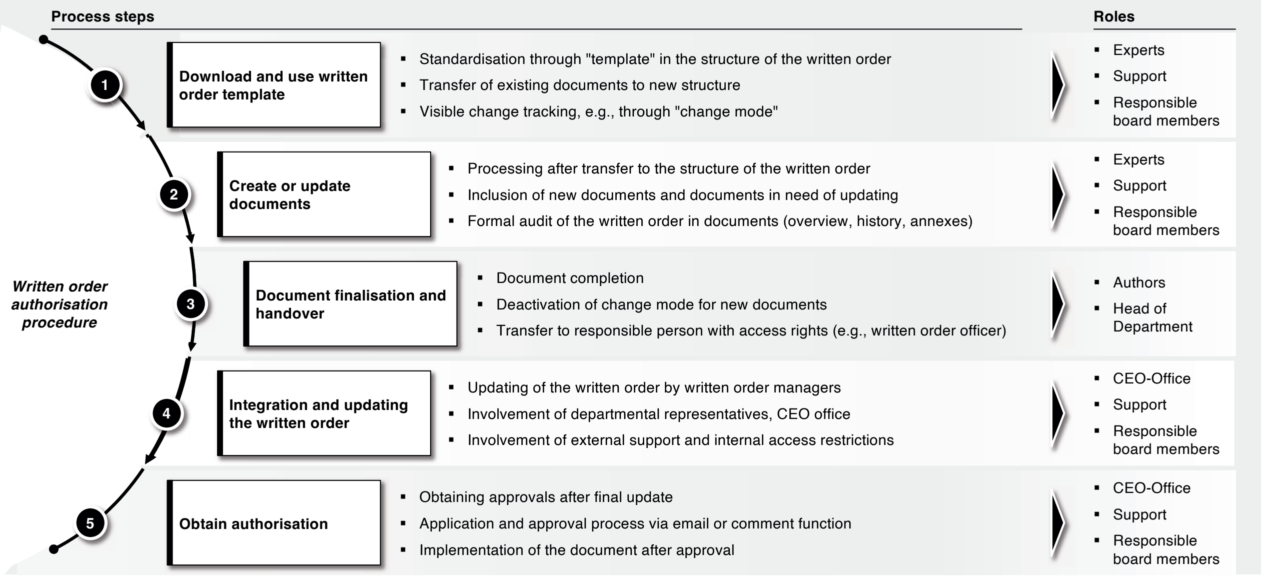
The objective is to transition the remaining findings of “low” and “medium” severity into regular operations and to close all findings. After the successful deregistration of the defect rectification by the supervised entity and the release by the auditor or the supervisory authority, long-term operational stability is to be ensured to maintain the ICT maturity of the organisation; this also includes preparation for a potential follow-up audit.

Approval process

Establishing and updating all documents should follow a systematic and controllable approach to guarantee traceability and transparency of alternators. It is recommended to delineate a fitting acceptance process that clearly defines requirements and responsibilities (Figure 16). Initially, a template for the written order should be set that contains all necessary information and requirements for all documents (e.g., document information, version history, uniform table of contents) and can serve as a basis for updates and the creation of new documents. Based on this, respective departments or experts can create documents and integrate existing documents into the template. After subsequent updates and creation of documents, the authors and experts should check whether the formal aspects of the written order are reflected in the document before handing them over to the written order’s responsible parties.

The written order's responsible parties (e.g., authorised departmental personnel, the CEO's office, or external support) incorporate the changes and begin the approval process. This application can be carried out in various ways, which should ensure that it is consistent, traceable, and transparent so that these documents can come into effect. For example, using comment functions in Confluence or laying down email evidence at appropriate points is advisable.

The written order is updated in accordance with a predefined approval procedure: steps and roles



Written order authorisation procedure

	Process steps		Roles
1	**Download and use written order template**	▪ Standardisation through "template" in the structure of the written order ▪ Transfer of existing documents to new structure ▪ Visible change tracking, e.g., through "change mode"	▪ Experts ▪ Support ▪ Responsible board members
2	**Create or update documents**	▪ Processing after transfer to the structure of the written order ▪ Inclusion of new documents and documents in need of updating ▪ Formal audit of the written order in documents (overview, history, annexes)	▪ Experts ▪ Support ▪ Responsible board members
3	**Document finalisation and handover**	▪ Document completion ▪ Deactivation of change mode for new documents ▪ Transfer to responsible person with access rights (e.g., written order officer)	▪ Authors ▪ Head of Department
4	**Integration and updating the written order**	▪ Updating of the written order by written order managers ▪ Involvement of departmental representatives, CEO office ▪ Involvement of external support and internal access restrictions	▪ CEO-Office ▪ Support ▪ Responsible board members
5	**Obtain authorisation**	▪ Obtaining approvals after final update ▪ Application and approval process via email or comment function ▪ Implementation of the document after approval	▪ CEO-Office ▪ Support ▪ Responsible board members

Source: Grey Swan Research Institute

Figure 16: Exemplary approval process for written order documents

It is important to emphasise that updating the written order is not a one-time process, but is carried out regularly and as needed. This allows for the identification of potential vulnerabilities and risks to ensure appropriate security within the company.

Fact-based reporting

By implementing unique identifiers for evidence and updating the defect rectification plan, a consistent overarching transparency is established. Coupled with recurring reporting, this solidifies success. Tracking the progress of each piece of evidence in a standardised format services as an early warning system. This system enables the identification of problem areas and the initiation of objective measures accordingly.

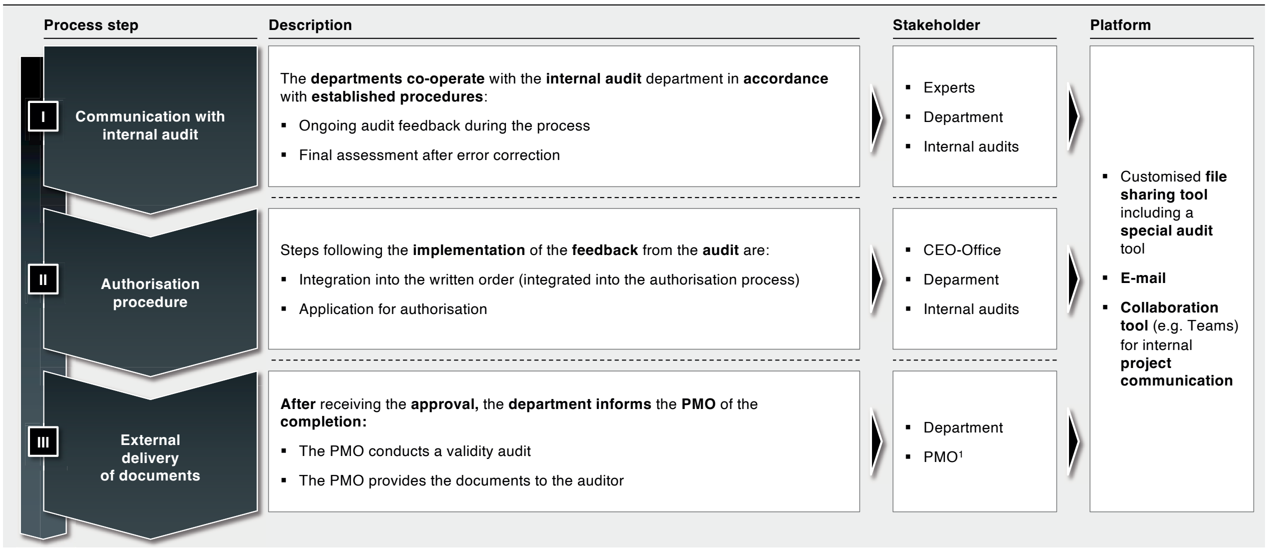
To simplify the assessment of evidence progress and avoid potential errors, it is advisable to develop a standardised reporting workflow tailored to findings and sub-findings, as well as a guide for reporting. Such a workflow includes different statuses with defined descriptions and a definition of the progress level, enabling standardised progress assessment across projects. If all evidence underlying a finding has the same status in the reporting, the finding (or sub-finding) inherits this status.

In the case of mixed statuses, the overall status inherits the lowest status of the evidence. The reporting can be broken down from a monthly to a bi-weekly or even weekly basis for management or an independent third party, thus enabling traceability.

End-to-end delivery process

The key to ensuring high-quality documents, regulatory-required filings, and fact-based reporting lies in an end-to-end delivery process. This process governs interactions with internal audit, the auditor, or external special representatives, as well as the responsible document authors, facilitating early feedback collection and coordination with internal audit for incorporation (Figure 17).

An end-to-end document delivery process ensures the creation of high-quality documents



Process step	Description	Stakeholder	Platform
I Communication with internal audit	The **departments co-operate** with the **internal audit** department in **accordance** with **established procedures**: ▪ Ongoing audit feedback during the process ▪ Final assessment after error correction	▪ Experts ▪ Department ▪ Internal audits	▪ Customised **file sharing tool** including a **special audit** tool ▪ **E-mail** ▪ **Collaboration tool** (e.g. Teams) for internal **project communication**
II Authorisation procedure	Steps following the **implementation** of the **feedback** from the **audit** are: ▪ Integration into the written order (integrated into the authorisation process) ▪ Application for authorisation	▪ CEO-Office ▪ Deparment ▪ Internal audits	
III External delivery of documents	**After** receiving the **approval,** the **department informs** the **PMO** of the **completion:** ▪ The PMO conducts a validity audit ▪ The PMO provides the documents to the auditor	▪ Department ▪ PMO[1]	

Source: Grey Swan I 1: PMO = Project Management Office

Figure 17: Document submission process

The interaction between departments and internal audit must follow specific guidelines, as internal audit serves as an independent evaluation body and not as a Quality Gate for individual documents. For this reason, after all deficiencies have been rectified, a formal audit opinion is created by the internal audit. To obtain approval or feedback for the rectified deficiencies, a prescribed approval process must be followed, in which the project team explicitly submits a request to internal audit along with all documents. Once approval is granted, the ultimate finalisation of the documents takes place.

The PMO conducts a plausibility audit and provides the documents to the special representative. Here, too, defined file-sharing tools and email systems are used to share documents securely and efficiently. This end-to-end delivery process enables departments, experts, the internal audit, and other stakeholders to create high-quality documents that are properly approved. Communication, responsibilities, and processes are essential for ensuring smooth collaboration and efficient document creation.

Verification of measures according to Test of Design, Test of Implementation, and Test of Effectiveness

Once measures are closed according to reporting, the next step will be verification of their effectiveness. This involves assessing the measures in terms of their planned implementation (Test of Design) as well as their actual effectiveness (Test of Effectiveness). The Test of Design checks whether the company's technical-organisational, legal, and personnel measures meet the requirements of legal provisions and are documented in the written order as a standard requirement. In addition to meeting the formalities of the written order, it is examined whether the necessary control and monitoring mechanisms to ensure compliance with legal requirements are in place. This includes, for example, audits on whether responsibilities, authorities, and competencies are regulated, whether sufficient internal controls and audit mechanisms exist, and whether compliance with internal guidelines and specifications is monitored by appropriate controls.

The ToX model (ToD, ToI, ToE) is essential for a successful project organisation for IT audits

The implementation test subsequently verifies the presence of controls that have been integrated into operational processes. It examines whether the measures defined in the written order are implemented according to legal and internal guidelines. Possible evidence for reviewing the implementation includes publications in the organisation's internal wiki, distribution/presentation at meetings, or confirmation of acknowledgment in the HR management tool.

The Test of Effectiveness (ToE) verifies whether the controls introduced in the Test of Implementation (ToI) have been effectively implemented according to their definition (ToD) and are effective in practice, e.g., function according to legal and internal requirements. The operationalisation of controls can occur in various dimensions, such as training personnel, providing communication proofs, and confirming effectiveness by internal or external auditors. To conduct the ToE, evidence reviewed by internal audit, which confirms the implementation of the controls, should be examined. The evidence should reflect the status of operationalisation to provide an overview of progress and identify possible deviations. It is important that the operationalisation of controls is continuously monitored and adjusted as needed. Overall, the ToE helps to identify weaknesses in the implementation of controls and, if necessary, initiate corrective measures to minimise the risk of errors and compliance violations.

Anchoring program management within the organisation as an additional success factor

Irrespective of the nature of the challenge – be it political, technological, or regulatory – experience demonstrates that mastering project and program management disciplines within the organisation is a key factor for success across the board. Three underlying success factors have been discussed for this mastery: methodological knowledge, tool support, and experienced experts. The last point is crucial for embedding project and program management within the organisation and offers three implementation options: insourcing, outsourcing, and hybrid (Figure 18).

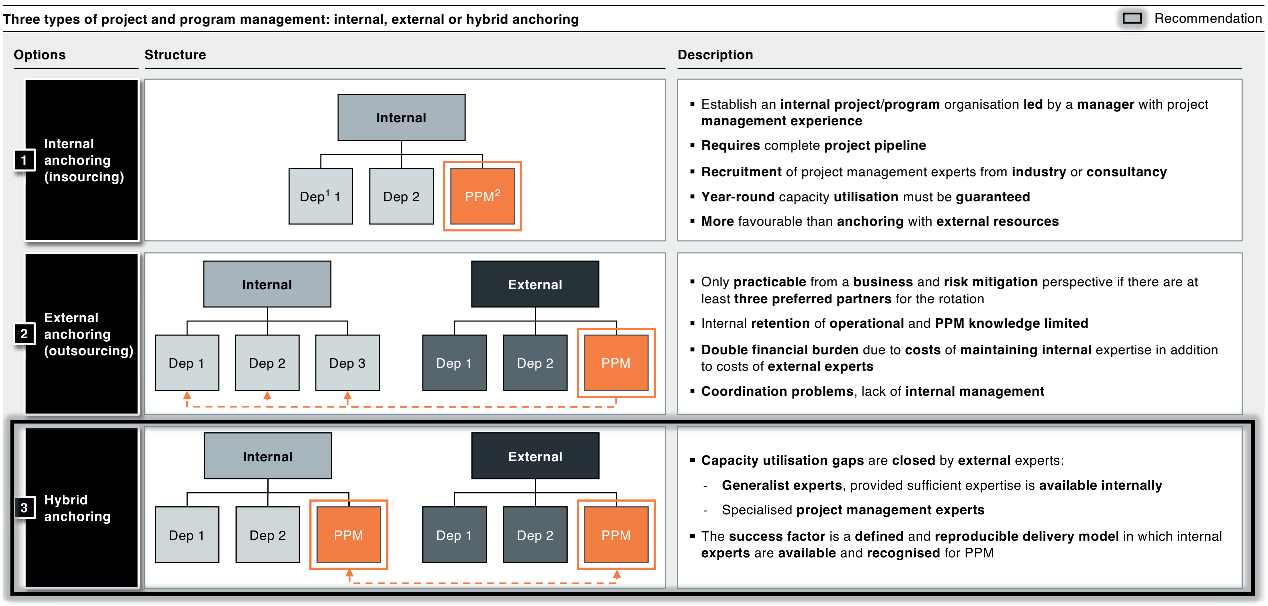
During an IT audit and when addressing deficiencies, it is advisable to ensure close integration of the project organisation with the established defence lines of the company, known as the Three

Lines of Defence model (LoD). Originally developed in the financial sector, this model describes a company's defence lines as follows:

- **1LoD:** Direct control is exercised by the business units and supporting service areas such as IT and Operations.

- **2LoD:** The role of the Information Security Officer (ISO) involves setting requirements, independently assessing information security risks, and conducting their own controls to monitor the implementation of measures by the first line of defence.

- **3LoD:** Internal Audit independently reviews the effectiveness of the Internal Control System (ICS) and other risk management processes, separate from the first two lines.



Three types of project and program management: internal, external or hybrid anchoring

□ Recommendation

Options	Structure	Description
1 Internal anchoring (insourcing)	Internal Dep[1] 1 · Dep 2 · PPM[2]	▪ Establish an **internal project/program** organisation **led** by a **manager** with project **management experience** ▪ **Requires** complete **project pipeline** ▪ **Recruitment** of project management experts from **industry** or **consultancy** ▪ **Year-round** capacity **utilisation** must be **guaranteed** ▪ **More** favourable than **anchoring** with **external resources**
2 External anchoring (outsourcing)	Internal: Dep 1 · Dep 2 · Dep 3 External: Dep 1 · Dep 2 · PPM	▪ Only **practicable** from a **business** and **risk mitigation** perspective if there are at least **three preferred partners** for the rotation ▪ Internal **retention** of **operational** and **PPM knowledge limited** ▪ **Double financial burden** due to **costs** of **maintaining internal** expertise in addition to costs of **external experts** ▪ **Coordination problems**, lack of **internal management**
3 Hybrid anchoring	Internal: Dep 1 · Dep 2 · PPM External: Dep 1 · Dep 2 · PPM	▪ **Capacity utilisation gaps** are **closed** by **external** experts: - **Generalist experts**, provided sufficient expertise is **available internally** - Specialised **project management experts** ▪ The **success factor** is a **defined** and **reproducible delivery model** in which internal **experts** are **available** and **recognised** for PPM

Source: Grey Swan I 1: Dep = Department I 2: PPM = Project and program management

Figure 18: Three forms of project and program management structures

Internal anchoring (Insourcing)

Internal anchoring involves establishing an internal project/program organisation, led by a manager with project management experience. For managing IT audits and defect rectification programs, it is vital that the project/program organisation possesses the necessary methodological knowledge, or that such knowledge is consistently developed, and that it is capable of understanding regulatory issues. This model requires a managed project pipeline and is comparatively cost-effective relative to using external resources. Implementation could be achieved by hiring former compliance experts, legal advisors, management consultants, and auditors. The model's potential weaknesses are ensuring year-round workload through projects from the operational business, which poses the challenge of balancing availability for ad-hoc scheduled audits against constant workload, and a reduction in flexibility due to permanent or fixed-term employments.

External anchoring (Outsourcing)

External anchoring is viable from a business management and risk mitigation perspective if there are at least three preferred partners bound by framework agreements. However, they must be available on a rotational basis for special projects, such as IT audits in accordance with XAIT, DORA, IT-SiG, etc., and subsequent elimination of defects. The potential breaking point in an outsourcing model lies in the regulatory requirement to maintain the necessary knowledge for operational capability internally. In the case of full outsourcing, this requirement would not apply. A further issue is the financial double burden, as internal knowledge retention is reflected in external experts. Ultimately, this option generates high costs, coordination efforts, and a lack of internal accountability.

Hybrid anchoring

Within the hybrid anchoring model, the workload gaps are filled by external experts. One way to close personnel gaps, assuming sufficient internal expertise is available, is to hire affordable and generalist external professionals. A second variant of the hybrid model involves the short-term hiring of specialised compliance and project management experts for audit situations, such as special audits or more complex defect rectifications. Key to success is a delivery model where internal experts are made available for audits and are marked in the human resource management software (e.g., Workday or Personio), as well as external experts being similarly identified for case-specific deployment.

The hybrid model represents a pragmatic approach

Summary

The performance of a business is significantly influenced by political, legal, and technological challenges. Professional management of the challenges at hand is critical to success and should therefore be organised as a project or program. For a project or program to be successfully implemented, it requires three key elements: methodological support, followed by tool support, and finally, the expertise of specialists in specific subject matters.

The execution of a complex program was illustrated using the example of an IT audit at financial institutions and operators of essential services (CRITIS) in Europe. These entities face an increasingly dense catalogue of vertical and horizontal requirements and must comply with these legal and technological demands.

IT audits are special situations for both the organisational structure and operational processes and can rarely be managed entirely by the line organisation. A special organisational structure for preparing and conducting the audit, as well as for rectifying deficiencies afterwards, must almost always be established. Companies typically resort to the addition of external expertise. In our view, the should be at parity, so that the expertise as required by the supervision can still be maintained internally, and vendor lock-in effects are avoided.

European critical infrastructures, specifically financial institutions are subject to a variety of cross-sector regulatory standards such as NIS2, CER, CRA, GDPR, and DORA. These extensive requirement catalogues result in a rise in IT audits for a greater number of companies. The introduction of the NIS2 Directive means that the number of companies monitored in Germany will rise from 2,000 to at least 30,000. By 2025, more than 22,000 financial institutions across Europe will be regulated under the DORA regulations; in Germany alone, the supervision will extend to over 3,600 financial institutions.

IT audits are increasingly becoming standard practice for companies. This regulatory objective is simultaneously a mandate for security policy, as the security organisation is continuously reviewed and improved. Further digitalisation transforms what is currently known as a “special audit” into a “continuous” audit. By adhering to defined, experience-based success factors for audit preparation, execution, and defect rectification, the audit outcome becomes predictable and less frequently results in severe sanctions.

A continuous audit occurs through automatically provided measurements and key indicators. This automation is a consistent continuation of digitalisation strategies for infrastructures, applications, and services. Thus, an audit is another digital service. This digitised offering is associated with positive feedback effects, as a largely automated audit requires a fully documented, risk-free, and seamlessly controlled monitored infrastructure. From this perspective, an IT audit no longer represents an operational disruption but is a tool for the upstream control and monitoring of one’s own infrastructure, a critical success factor for the timely and effective implementation of defect rectification, and a pioneer of a digitally performant production platform that allows more room for core business activities.

Sources

1. European Council. (2024). *Sanctions. European Council. Retrieved from https://www.consilium.europa.eu/de/policies/sanctions/*

2. European Union. (03.2024). *EU sanctions tracking. Europe Analytics. Retrieved from https://data.europa.eu/apps/eusanctionstracker/*

3. Leisering, K. (02.01.2024). *EQS. Retrieved from https://www.eqs.com/compliance-blog/eusupply-chain-law/*

4. McFarland, A. (11.2023). *Unite AI. Retrieved from https://www.unite.ai/oreilly-generative-aiin-the-enterprise-2023-report/*

5. Gartner. (13.12.2022). *gartner.com. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2022-12-13-gartner-forecasts-worldwide-low-code-development-technologies-market-to-grow-20-percent-in-2023*

6. Gartner. (12.2022). *Gartner Worldwide Market for Low-Code Development Technologies in2023 [Press release]. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2022-12-13-gartner-forecasts-worldwide-low-code-development-technologies-market-togrow-20-percent-in-2023*

7. Bank for International Settlements (BIS). *(n.d.). Basel III: international regulatory framework for banks. Retrieved from Bank for International Settlements (BIS): https://www.bis.org/bcbs/basel3.htm*

8. BaFin. (10.2023). *Circular 05/2023 (BA) - Minimum requirements for risk management - MaRisk. Retrieved from https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2023/rs_05_2023_Ma-Risk_BA.html;jsessionid=2278012D386A911119744E387A86E492.internet001?nn=19659504 abgerufen*

9. European Commission. (2022). *Proposal of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and on the amendments to Regulation (EU) 2019/1020. Brussels: European Commission.*

10. European Commission. (2016). *General Data Protection Regulation. Brussels: European Commission.*

11. European Commission. (2022). *Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience in the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Brussels: European Commission.*

12. European Commission. (2022). *Directive (EU) 2022/2464 of the European Parliament and of the Council amending Regulation (EU) No 537/2014 and Directives 2004/109/EC, 2006/43/EC and 2013/34/EU as regards corporate sustainability reporting. Brussels: European Commission.*

13. United Nations. (n.d.). *United Nations - Department of Economic and Social Affairs Sustainable Development. Retrieved from https://sdgs.un.org/goals*

14. Global Reporting Initiative. (n.d.). *Global Reporting Initiative. Retrieved from https://www.globalreporting.org*

15. U.S. Securities and exchange commission. (25.09.2023). *U.S. Securities and exchange commission. Retrieved from https://www.sec.gov/news/press-release/2023-194 New Order I White paper I 2024 I © Grey Swan 27*

16. sanction scanner. (2023). *Financial Crime & Compliance. Retrieved from Sanction Scanner: Retrieved from https://sanctionscanner.com/Content/Report/2023-2024-Financial-Crime-and-Compliance-Report.pdf*

17. Kröner, A., & Schwarz, D. (01.2023). *Financial regulator restricts new business of fin-tech Solaris. Retrieved from Handelsblatt https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/bafin-finanzaufsicht-schraenkt-neugeschaeft-von-fintech-solarisein/28922928.html*

18. Handelsblatt. (2023). *Smartphonebank: Bafin extends conditions against N26 - Fintech may continue to grow only to a limited extent. Retrieved from https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/smartphonebank-bafin-verlaengert-auflagen-gegen-n26-fintech-darf-weiterhin-nur-begrenzt-wachsen/29238276.html*

19. Deutsche Bank. (09.11.2020). *Deutsche Bank sells Postbank Systems to Tata Consultancy Services. Retrieved from Deutsche Bank: https://www.db.com/news/detail/20201109-deutschebank-announces-sale-of-postbank-systems-to-tata-consultancy-services?language_id=3*

20. Deutsche Bahn. (2022). *From Digitalisation projects and concepts in focus. Retrieved from https://ibir.deutschebahn.com/2022/de/konzernlagebericht/produktqualitaet-und-digitalisierung/digitalisierung/digitalisierungsprojekte-und-konzepte-im-fokus/*

21. Handelsblatt. (2024). *Handelsblatt. From Artificial intelligence - Vodafone joins forces with Microsoft. Retrieved from https://www.handelsblatt.com/technik/ki/kuenstliche-intelligenz-vodafone-verbuendet-sich-mit-microsoft/100007448.html*

22. Handelsblatt. (01.2024). *Handelsblatt. Retrieved from https://www.handelsblatt.com/technik/ki/tech-leitmesse-ces-2024-siemens-verbuendet-sich-mit-amazon-fuer-ki-partnerschaft/100005372.html*

23. Market Screener. (2023). *Toshiba. Retrieved from https://de.marketscreener.com/kurs/aktie/TOSHIBA-6493713/news/Japan-Industrial-Partners-Inc-ROHM-Co-Ltd-TSE-6963-und-Suzuki-Motor-Corporation-TSE-7269-ha-44894603/*

24. Microsoft. (03.2022). *Microsoft completes acquisition of Nuance, ushering in new era of outcomes- based AI. Retrieved from https://news.microsoft.com/2022/03/04/microsoft-completesacquisition- of-nuance-ushering-in-new-era-of-outcomes-based-ai/25. European Banking Authority. (01.2024). European Banking Authority. Retrieved from EBA's mission and tasks. Retrieved from https://www.eba.europa.eu/deutsch*

26. European Insurance and Occupational Pensions Authority. (6.02.2023). *European Insurance and Occupational Pensions Authority. Retrieved from https://www.eiopa.europa.eu/media/events/joint-esas-public-event-dora-technical-discussion-2023-02-06_en?prefLang=de&etrans=de*

27. European Securities and Markets Authority. (January 2024). *European Securities and Markets Authority. Retrieved from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-securities-and-markets-authority-esma_de*

28. Federal Office for Information Security. (2023). *What are Critical Infrastructures. Retrieved from https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis.html*

29. European Parliament and Council of the European Union. (2022). *NIS 2 Directive. Brussels: Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555&qid=1705010003184*

30. European Parliament and Council of the European Union. (2016). *NIS Directive. Brussels: Official Journal of the European Union. New Order | White paper | 2024 | © Grey Swan 28*

31. German Bundestag. (2021). *Supply Chain Due Diligence Act (LkSG). Berlin: Federal Law Gazette.*

32. Dimensional Research, Netenrich. (2021). *Pivoting to Risk-Driven and Proactive Security. Retrieved from https://netenrich.com/hubfs/web/resources/netenrich-pivoting-to-risk-drivensecops-executive-brief.pdf*

List of abbreviations

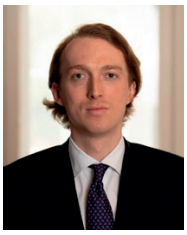
Abbreviation	Description
1LoD	First line of defence
2LoD	Second line of defence
3LoD	Third line of defence
AI	Artificial Intelligence
BAIT	«Bankaufsichtliche Anforderungen an das IT» (Banking supervisory requirements for IT)
CER	«Critical-Entities-Resilience-Richtlinie» (Critical Entities Resilience Directive)
CRA	Cyber-Resilience-Act
CRITIS	Critical infrastructure
CSDDD	«EU-Lieferkettenrichtlinien 2022» (EU Corporate Supply Chain Due Diligence Directive 2022)
CSRD	«EU-Richtlinie zur Unternehmens-Nachhaltigkeitsberichterstattung» (EU Corporate sustainability reporting directive)
DORA	«Verordnung zur Digitalen Operativen Resilienz» (Regulation on Digital Operational Resilience Act)
DSGVO	«Datenschutz-Grundverordnung» (General Data Protection Regulation)
DWS	«Deutsche Gesellschaft für Wertpapiersparen» (German Society for Securities Savings)
ESG	Environmental, social and governance
GRI	Sustainability reporting
IaaS	Infrastructure as a service
ISMS	Management system for information security
IT	Information technology

Abbreviation	Description
IT-SiG	«Informations-technologisches-Sicherheitsgesetz» (Information Technology Security Act)
KAIT	«Kapitalverwaltungsaufsichtliche Anforderungen an die IT» (Capital management supervisory requirements for IT)
KPI	Key performance indicators
MaRisk	«Mindestanforderungen an das Risikomanagement» (Minimum requirements for risk management)
NIS1	«Netzwerk-Informationssicherheits-Richtlinie 1.0» (Network Information Security Policy 1.0)
NIS2	«Netzwerk-Informationssicherheits-Richtlinie 2.0» (Network Information Security Policy 2.0)
PaaS	Platform as a service
PMO	Project Management Office
SaaS	Software as a service
SDG	«United Nations-Nachhaltigkeitsziele» (United Nations sustainable development goals)
SDLC	Software development life cycle
SEC	United States Securities and Exchange Commission
SME	Subject Matter Expert
ToD	Test-of-Design
ToE	Test-of-Effectiveness
ToI	Test-of-Implementation
VAIT	«Versicherungsaufsichtliche Anforderungen an die IT» (Insurance supervisory requirements for IT)
XAIT	Collective term for BAIT, KAIT, VAIT, ZAIT
ZAIT	«Zahlungsdienstlicheaufsichtliche Anforderungen an die IT» (Payment service supervisory requirements for IT)

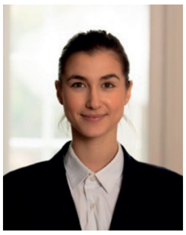
Authors

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.

Julius Düwel is a Manager at Grey Swan, holding a master's in management from IE Business School. He has extensive experience in IT consulting, focusing on program management, risk strategy development, and compliance management. He led programs for special audits in the banking sector, business impact analyses and feasibility studies for core banking systems.



Pauline Schmidt is an Associate Consultant at Grey Swan. She is an expert in ESG (Environmental, Social & Governance) and project management, with a focus on promoting sustainable corporate governance. She holds a Bachelor of Arts in Business Administration with a specialisation in Sustainability Management from the University of Applied Sciences in Berlin.



Tamino Müller is a Fellow Consultant at Grey Swan. During his studies at a London business school, he gained experience as a business analyst and consultant for Fortune 500 companies. With a focus on finance, he supports the risk, finance, and program management teams. His experience includes credit process and treasury optimisation for banks.

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

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

April 2024