

---

# Business Solutions Guide: Compliance by Design Five Rules To Reduce Risk For Application Landscapes

## Business Solutions Guide: Compliance by Design. Five Rules To Reduce Risk For Application Landscapes

This guide is for people responsible for ensuring the security and compliance of enterprises' application landscapes, including CIOs, CISOs, Heads of IT Governance as well as enterprise architects. It sets out five rules for creating a future IT landscape that infringes neither internal nor external regulations and delivers business value.

### Avoiding the tabloids

One of the most reliable ways for an enterprise to get media coverage is to have a spectacular IT security leak.

While organizations spend a great deal on risk analysis of their applications to avoid such headlines, news about the loss of customer data or the hacking of security systems still regularly hits the wires. Even when there are established internal regulations, they are often simply not enforced – which shows just how difficult it is to close all security holes – especially when facing increasing complexity and decreasing IT budgets.

*“You are constantly forced to think about how you could reduce the complexity, where to start and whether the business will comply. And what does this reduction mean?” says Klaus Wolf, Director of IT Management at Generali Deutschland Informatik Services.*

External regulations add to the complexity. Since decision makers may be made personally liable for the compliance of their application landscape, it is no surprise that organizations take this task very seriously and put a lot of effort into the landscape's yearly health-check.

The best way of passing the test is to maintain a healthy lifestyle on an organizational level, which requires the implementation and automation of effective IT governance processes. Organizations that manage to combine the decision processes of IT risk and compliance management with the ongoing evolution of their IT portfolios will get most out of their IT GRC initiatives.

We hope this guide will help you. It provides five rules for implementing compliance by design, from exposing IT risks to designing a future IT landscape that powers business success. Please contact us to discuss any of the issues raised.

## Rule 1: Catch up with reality.

To understand existing risks and compliance gaps you need a deep insight into your current application landscape.

What many organizations accept as their “current landscape” is quite often nothing but a mirage from the past. A recent study from Nucleus Research found that enterprise IT decision makers rely on information that is, on average, 14 months old – and only 55% accurate. This creates a severe data quality issue for any risk or compliance related analysis. In contrast, organizations that can truly trust their data can make decisions with much greater confidence.

*“Now we have consistency in the data and the relationships to make sure we can do the analysis correctly. And the ability to refresh our asset inventories like processes, applications, platforms, business objects, etc., of course, that’s very important. Confidence levels go way down for rationalization or analysis if data’s not fresh and current,” says Gabriel Morgan, Principal Enterprise Architect at MSIT.*



Thus, before assessing or analyzing an application landscape’s risk exposure or compliance gaps, organizations have to catch up with reality and make sure they have real-time insight into their IT portfolio.

## Rule 2: Make it a routine.

Given the sheer volume of information and the dynamics of ongoing changes, data collection itself cannot be handled en masse, on-demand anymore.

Nevertheless, many organizations use a compliance audit or a risk analysis as a trigger for interviewing application managers and other IT personnel on the status of the existing application landscape. This can happen repeatedly if several audits occur, thus creating multiple inconsistent snapshots of a constantly changing IT environment.

*„The platform is used by stakeholders across Credit Suisse’s global organization dealing with 3000 applications including 3000 technical components and their relations to each other,“ stresses Stephan Hug, CTO, Private Banking IT at Credit Suisse.*

The only way to get an accurate, real-time view of the current IT landscape is to ensure that all changes are carefully tracked and that the information is permanently updated with as much automation as possible. Still, this cannot be done by one person alone or even by a dedicated team. It needs to become a routine for everyone who alters the landscape to report changes, when they are made. In other words, all do some instead of some do all.

## Rule 3: Avoid silos.

Most organizations drive risk evaluation or compliance audits from distinct organizational units – which is fine. But those often create and maintain separate data sources – which is not fine.

A siloed approach where data on the IT landscape and the business context is stored separately from risk and compliance relevant information and where planning of changes and mitigation actions takes place in yet another environment, produces inconsistent views and enormous costs. And it leaves plenty of room for misinterpretation and blind spots.

*“A centralized information base is fundamental for managing the development, optimization and operation of the application landscape,“ says Klaus Wolf, Director of IT Management at Generali Deutschland*

---

*Informatik Services. “Many IT processes – not just ITIL or CMMI – can be supported by an active repository, and can also be created in such a way that the latest project information will feed directly into your planning,” continues Wolf.*

Only an integrated IT portfolio with insight into all aspects of the IT landscape as well as planned changes allows a comprehensive analysis of existing as well as future risks and compliance gaps. Nucleus Research<sup>1</sup> finds in one of their recent reports that by bringing all the data into one consistent repository with business, budgeting, and architecture framework support you arrive at one single source of the truth.

#### Rule 4: Automate the processes.

Manually managed processes are error-prone, costly and often very slow. This is especially true for complex processes that involve many stakeholders.

Managing compliance and risk of an application landscape requires complex IT governance processes to update, synchronize and connect the relevant data, plans and stakeholders while complying with internal objectives and external regulations. The automation of these processes thus offers great potential to increase both their efficiency and effectiveness.

*“A repository defines the controls for all these processes,” says Wolf from Generali. “Now the governance projects are working to these controls, and it is easy to request, for example, a SAS70 report.” Jan Rick, former Head of IT Strategy at Deutsche Bahn, assists: “The implementation of this kind of planning software and its potential for improving the IT processes is a good long-term investment.”*

Automated workflows ensure that all steps of a process are executed correctly and that their status can be tracked. This level of transparency is essential in the oversight of risk and compliance assessments as well as in mitigation planning, especially since both tasks require a multitude of cross-departmental, synchronized interactions.

## Rule 5: Comply by design.

Uncovering a risk or a compliance gap in the existing IT landscape is the result of a good analysis – and of bad planning.

Many organizations relegate the task of risk and compliance analysis to an afterthought of an IT landscape's evolution instead of making it an integral part of their IT planning efforts. This is rarely done with intention; it is rather a consequence of lacking the information needed to anticipate the impact of changes at design-time. Having this information makes all the difference, enabling decision makers to identify gaps and avoid them in time.



*“It’s very important that we direct our investments to move on from [outdated] platforms at the most critical, the most important points, so we can replace them appropriately. We want to minimize our risk, so knowing which business processes those applications are privy to, making those investments and moving on are incredibly important to us,” says the Head of Enterprise Architecture at a global player in the oil & gas industry.*

Following rules one through four, enables organizations to move some of the assessment and analysis effort upstream and run it already at design time. Thus, all the actions can be aligned with the organization's risk appetite and compliance obligations in order to avoid security leaks, penalties and unnecessary mitigation loops downstream. This ultimately paves the way for an organization to achieve compliance by design.

## Conclusion

Compliance is less a matter of testing than a matter of implementation. The same is true for IT risk management. They both depend on the consistency of information and the transparency of execution – an objective that IT governance pursues.

Business IT Management means to implement and automate IT governance. It is the task of ensuring that IT powers business success while complying with internal and external regulations. It combines a deep understanding of the business and its strategy with the insight, planning and execution required to evolve the IT landscape. The five rules provide a comprehensive approach to get to grips with compliance and risk through Business IT Management.

alfabet is the only vendor that has a comprehensive software suite that supports all aspects of Business IT Management – from real-time insight into the enterprise architecture to forecasting, risk management, compliance, roadmapping and execution.

### **About alfabet ([www.alfabet.com](http://www.alfabet.com))**

Business IT Management is the task of ensuring that IT powers business success. It combines a deep understanding of the business and its strategy with the insight, planning and execution required to evolve the IT landscape. alfabet is the only vendor providing a comprehensive software suite that supports all aspects of Business IT Management – from accurate insight into the enterprise architecture to IT planning, risk management, compliance, road-mapping and IT Program Control.

alfabet serves with its flagship product planningIT ® a global user community of more than 135,000 IT, Finance and Business professionals in more than 40 countries. Customers of alfabet include many of the Global 2000 companies across a broad range of industries in particular financial services, automotive, telecommunications, logistics, and high-tech.

Founded in 1997, alfabet is operating with headquarters in Berlin, Cambridge, Mass and Singapore.