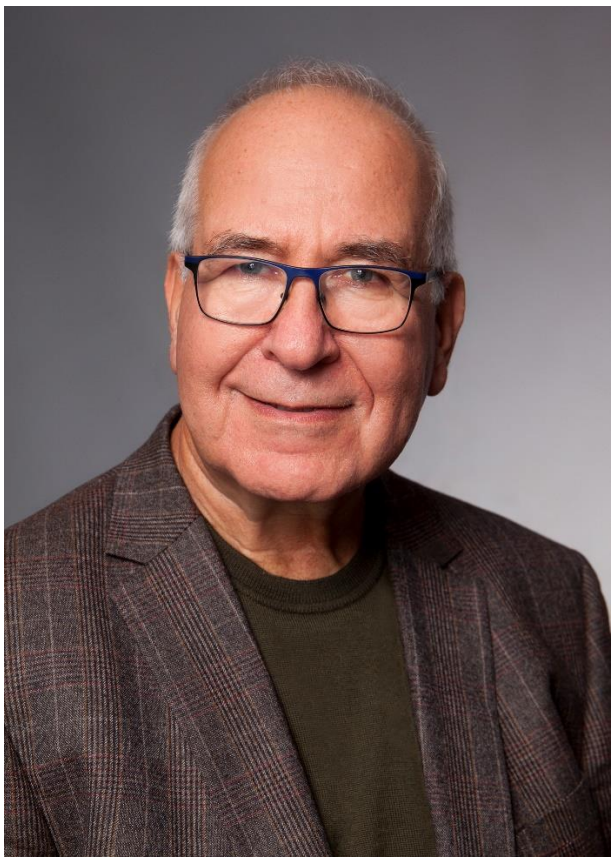
Balancing Agility and Resilience through Visibility, Trust and Automation



Kristof Kloeckner

Technology Executive | Advisory Board Member

Enterprises are facing a perfect storm of increased risks and opportunity. With rapidly changing business environments and heightened risks to their operations and supply chains, they need to reassess whether their processes and structures are agile enough to adapt and to grasp opportunities, and at the same resilient enough to dealt with disruption and cope with unforeseen catastrophic events.

They do not have the luxury to focus on either agility or resilience exclusively. Without agility, they risk atrophy and will miss opportunities, while fragility due to lack of resilience threatens damage that might imperil any gains. The Covid-19 pandemic, the horrible reality of wars and the increase of cyberthreats have exposed weaknesses in societies and enterprises, often due to having overoptimized for efficiency over resilience. This applies to both the physical and the digital world.

Balancing agility and resilience requires a structured approach and an economic model for assessing risks and rewards.

In the following, I would like to focus on the IT underpinnings of digital transformation and suggest an approach that has been updated from early times of service management. It looks at architecture or structure of IT systems, the processes to manage their lifecycle and best practices for both.

The principles for successful service management that we defined in the early 2000s build on each other:

- Visibility
- Control
- Automation

Visibility means full understanding of the state of your system. Extending the original concept of visibility to include observing a system's behavior and its changes, and to understanding the relevance of data in context leads to the concept of **observability**, which has been introduced in the context of application management. This extended visibility is the underpinning of everything else, especially in the face of rapid change.

Control is the ability to ensure that policies (and best practices) are followed throughout the lifecycle, from development to deployment to change. It is imperative that control systems can be trusted, are transparent to people with a need to know and are secure (for instance, tamper-proof). **Trust,** if it is not naïve, implies verification and control.

Finally, the size and complexity of systems, the speed of change and the volume of events affecting the system require any management system to be **automated**. Automation needs to be trusted in order to be accepted by stakeholders. Essentially, this means its workings need to be understandable and verifiable. These requirements open up a number of

challenges for AI-driven automation that are being addressed through initiatives for ‘trustworthy’ or ‘explainable’ AI. This topic will not be addressed here.

In light of the importance of keeping up with rapid change and achieving and maintaining trust, I would like to update the original set of principles to

- **Visibility**
- **Trust**
- **Automation**

I will discuss how to apply these principles to digital transformation and hybrid cloud.

Enterprises in all industries are pursuing digital transformation, adopting new business models and introducing new services. The pandemic has exacerbated this trend. In a 2020 study by KPMG, 74% of surveyed CEOs see an acceleration of ‘the digitization of operations and the creation of a next-generation operating model’ [1]. This introduces more dependencies on their IT infrastructure and its supply chain. Business cycles are compressing and macro-economic risks are increasing, the mix of services an organization consumes and provides is getting more complex and potentially more vulnerable.

They need to decide which services to retain, rework or replace, where to source new services and components, how to deploy and manage them, and how to integrate it all to provide a superior user experience to clients and customers. A hybrid cloud approach is taken by the vast majority of enterprises. According to a 2021 study by the IBM Institute for Business Value, 97% of surveyed customers have a mix of public and private clouds, 59% have multiple public clouds [2].

It is imperative that a business has full **visibility** of its application landscape and the supporting infrastructure and is able to **trust** this information and to put it into a business context. Achieving visibility is becoming difficult with a shift from static, centralized systems and organizations (mainframe or large Unix systems, exclusively in-house development) to

more distributed and dynamic structures (multi-cloud, containers and micro-services, complex software supply chains using open source).

- Provenance, quality and vulnerability of an organization's software components need to be established in a trustworthy and tamper-proof way with a framework that puts the overall risk in the context of its business goals. There are important community-based initiatives like the Open Web Application Security Project (OWASP) addressing the software supply chain and defining standards for Software Bills of Material, as well as Vulnerability Databases and early adopters are making use of this. US Executive Order 1408 gives explicit guidance on the security of software supply chains [3].

- Composition and dependencies of services need to be fully understood end-to-end, and behavior needs to be observable in order to ensure quality of service. A systematic approach to application performance management is needed.

- The portfolio of business services needs to be understood from both a business value and implementation point of view. Are existing enterprise (legacy) applications performing well and can they be integrated with new services? In that case, retaining and evolving them may be preferable to replacement. It reduces risk, since operational practices are established already, and it allows resources to focus on other needs. If these applications are well structured, they can quite easily expose their interfaces as APIs, often these APIs can be generated through tools. According to a 2020 Forrester Study, 74% of respondents expect the mainframe to have long-term viability as a strategic platform for their organizations [4], so integration tools and practices are needed.

- Cost and efficiency of service deployment needs to be transparent, including the choices of cloud service providers or a decision to retain a service in-house.

- It’s important to be able to assess the overall fitness of the service architecture, for instance understanding if there are single points of failure, performance bottlenecks or other architectural limitations to scale or robustness. How would the system cope with unexpected workload volumes or cyber threats? Can the architecture evolve to serve future business needs? Using pattern-based approaches, reference architectures and best practices frameworks can greatly help this task. All the major cloud providers are providing tools and assets in this space.

Once a baseline of visibility is achieved, an organization can apply policies and determine what controlled changes are needed and viable. The basis for the trade-offs may vary with changing business environments. A service-oriented architecture and ultimately micro-services will provide more flexibility and agility than monolithic approaches. It may make sense to break up existing monoliths in an incremental fashion, for instance using a strangler pattern.

Finally, both establishing the baseline and transforming it cannot rely on static manual control systems anymore. It requires trusted **automation** to manage complexity, scale and volume at speed. The following short, non-exhaustive, list can illustrate this.

- Application topology discovery replaces static CMDBs and allows effect application performance management based on the concept of observability

- Code scanners, dependency trackers and SBOM generators can automate the task of creating a baseline for vulnerability assessment and staying ahead of configuration drift.

- Service automation, in particular incident management automation can accelerate processes and eliminate human error.

- Automatic generation of APIs through an API factory can unleash the potential of existing enterprise application and enable integrating them into cloud native contexts.

In summary, applying the principles of visibility, trust and automation to transformation and management of hybrid cloud environments allows balancing resilience and agility. It should be complemented by organizational transformation and adoption of lean and agile lifecycle practices like Scaled Agile, DevSecOps and Site Reliability Engineering.

References and Acknowledgements

I would like to thank Gerd Breiter and Sal Vella for some valuable insights.

[1] https://home.kpmg/us/en/home/insights/2020/09/digital-acceleration.html, accessed 7/1/22
[2] https://www.ibm.com/thought-leadership/institute-business-value/report/cloud-transformation, accessed 7/1/22
[3] https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-supply-chain-security-guidance, accessed 7/1/22
[4] https://www2.deloitte.com/us/en/pages/consulting/articles/hello-mainframe-thank-you.html, accessed 7/1/22