From Technology Decision to Strategic Control

Executive Summary
The latest Highly Resilient Organisations (HRO) session brought together 18 CISO's to address a fundamental shift in how organisations must approach cloud infrastructure. The discussion, featuring insights from Michiel Steltman and Marc Welters, facilitated by Suzanne Janse, revealed that cloud adoption has evolved from an efficiency-driven IT decision to a board-level strategic imperative centred on digital sovereignty and control.

In today's geopolitical and regulatory landscape, the question is no longer simply about optimising costs and maximising uptime. Instead, boards confront a more fundamental challenge: who ultimately controls their organisation's digital assets and operational continuity? This session explored how digital sovereignty has emerged as a critical strategic asset, with implications that reach far beyond the IT department.

Context: The shifting cloud paradigm
For over a decade, cloud adoption was predominantly driven by promises of efficiency, scalability, and cost optimisation. Organisations eagerly migrated workloads, attracted by reduced capital expenditure and operational flexibility. However, the era of cloud enthusiasm is ending. Recent geopolitical tensions, regulatory developments and market concentration have transformed cloud infrastructure from a purely technical consideration into a matter of strategic autonomy and related risks.

The session highlighted how organisations must now balance the undeniable benefits of cloud services with the imperative to maintain control over their digital assets. This balance requires a sophisticated understanding of dependencies, risks and the true cost of geographical vendor lock-in, not just in financial terms, but in strategic flexibility and operational sovereignty.

The sovereignty challenge: personal and organisational
Suzanne set the scene (as usual) with a piece of contemporary art. Julia Janssen's "0.014 Seconds" provides a powerful metaphor for the sovereignty challenge. Her reading performance of thousands of pages of legal text triggered by one single "accept cookies" click illustrates how both personal and organisational sovereignty rest upon mountains of invisible contracts and complex dependency relationships. This artistic interpretation resonated with participants, highlighting how seemingly simple decisions create binding obligations with far-reaching implications.

> Risk (not rule) based is the way to go: determine risks on a case-by-case basis, mitigation is challenging, resilience to any pressure is key
>
> 
>
> **Michiel Steltman**
> Independent expert digital society

Sovereignty leverage: clear exit strategies
Michiel Steltman set the stage with an enthusiastic presentation about the importance of principle based approach to sovereignty risks. The ability to disengage from a cloud provider has emerged as the ultimate measure of digital sovereignty. Organisations that cannot exit due to technical complexity, contractual obligations or data gravity have effectively outsourced their strategic autonomy. This lock-in creates asymmetric power dynamics where providers hold disproportionate influence over an organisation's operational future.

CISOs must work with their boards to establish clear exit strategies that go beyond theoretical planning. This includes maintaining technical capabilities for workload portability, ensuring contractual terms permit disengagement, and regularly testing migration procedures. The goal is not necessarily to exit, but to ensure that the option remains viable, while maintaining negotiating power and strategic flexibility.

Resilience reporting: digital risks are becoming material
Digital continuity has evolved into a material risk requiring formal governance and external reporting. "Each organisation should determine such risks on a case-by-case basis to determine its ultimate materiality, even though its mitigation is challenging", according to Michiel. Boards can no longer treat IT resilience as just a technical metric in operational reports. Instead, they must evidence, govern and communicate their digital resilience posture to stakeholders, regulators and markets.

The International Digital Reporting Standards (IDRS) framework offers such a structured approach to transparency, enabling organisations to demonstrate their resilience capabilities systematically. This shift toward standardised reporting reflects the growing recognition that digital infrastructure underpins in general all major business operations and must be governed accordingly. One of the CISOs of a large Dutch

international organisation explained: “We have seen such geopolitical risks for many decades and survived many crises and even wars. By spreading the risks among countries, entities, decentralised systems and multiple (back-up) suppliers we aim to minimise the material impact of major incidents.”

End-to-end dependencies: hidden risks
Cloud related risks extend far beyond primary service providers. The session emphasised how hidden sub-processors and dependencies through third, fourth, and even fifth parties create complex risk webs that most organisations struggle to map and manage. These invisible dependencies can create unexpected single points of failure or regulatory exposure. Organisations must develop capabilities to trace and assess their complete dependency chains. This requires going beyond traditional vendor management to understand the entire ecosystem supporting all digital operations. Geographic distribution of third, fourth and fifth parties and regulatory jurisdictions all contribute to an organisation’s true risk profile.

Exit readiness: strategic insurance in uncertain times
The ability to move workloads between providers or back on-premises is no longer optional redundancy, it is a strategic insurance. Regulatory shifts, geopolitical tensions, sanctions and provider failures can all trigger the need for rapid infrastructure changes. Organisations without exit readiness face potential operational paralysis when these scenarios materialise. This readiness requires continuous investment in multi-cloud capabilities, data portability standards and architectural decisions that prioritise flexibility over optimisation. While this approach may increase short-term costs, it provides essential protection against long-tail risks that could prove existential.

Scenario planning: testing strategic resilience
Boards must engage in rigorous scenario planning that tests their digital sovereignty under stress. This includes modelling geopolitical escalations, regulatory interventions, provider failures and market consolidation. Understanding where control holds or breaks under these scenarios enables proactive risk management and strategic positioning. These exercises should move beyond technical failure scenarios and include strategic and geopolitical crises. What happens if a provider becomes subject to foreign sanctions or is being ringfenced due to a local war? How would new data localisation requirements impact operations? Where do dependencies become really material to business continuity?

IDRS provides boards with a transparent, standardised way to measure and evidence digital control, making sovereignty a governable and reportable capability rather than an abstract concept

Marc Welters
Partner IT Audit and IT Advisory at EY

Julia Janssen’s artwork “0.014 Seconds” provides a powerful metaphor for the sovereignty challenge and illustrates how both personal and organizational sovereignty rest upon mountains of invisible contracts and complex dependency relationships.

Suzanne Janse
Lecturer and research supervisor at Erasmus Economics & Business Executive Education

Conclusion
Organisations that recognise digital infrastructure as a sovereign asset requiring active governance will be better positioned to navigate increasing uncertainty. Boards must elevate cloud strategy from a technology decision to a strategic imperative, ensuring their organisations maintain the flexibility and control necessary for long-term resilience and even existence. “IDRS is a promising way to provide boards with a transparent, standardised way to measure and evidence digital control. It makes sovereignty a governable and reportable capability, rather than an abstract concept”, according to Marc Welters.