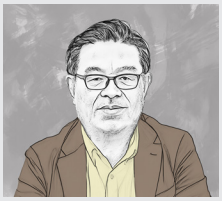
THE
kyndryl
institute

Trend Topic: **Governance Risk and Compliance in the Age of AI**

By



Dr Jun Murai

Co-Director of the Cyber Civilization Research Center, Keio University

Dr Jun Murai is Co-Director of the Cyber Civilization Research Center at Japan's Keio University. Dr Murai is a founding member of International Cybersecurity Center of Excellence and is widely recognized as 'the father of the internet in Japan' for his pioneering role in building and expanding networks across the country and Asia.

Explore more from The Kyndryl Institute
kyndryl.com/institute

Connection is resilience

When I first built the Japan University Network JUNET as a student in 1984, it was a computer network that originally connected the University of Tokyo, the Tokyo Institute of Technology and Keio University, and it was a network for ourselves.

In 40 years, it has evolved to become something for everyone, for the world, but what remains the same is that at its heart lies the power of connection. And now that critical infrastructures are connected through the internet, the goal of cybersecurity is not just to protect systems but to build a safe society. That future will be shaped by connected companies, connected societies, and a connected world. Key to this is standardization and collaboration.

Connection across all industries saves lives

As society digitizes, OT (Operational Technology) and IT (Information Technology) have merged. If this connection is not seamless and secure, vulnerabilities arise. On January 2, 2024, a Japan Airlines Airbus collided with a Coast Guard aircraft at Haneda Airport in Tokyo. The system detected the runway intrusion, but the control tower missed it – a human error at the OT-IT interface. This is precisely a fraying at the seam between OT and IT, and as the world of OT – once managed by seasoned experts

like air traffic controllers – integrates with digital systems, the central question for cybersecurity has become how to safeguard safety in this convergence. The vulnerability comes from the fact that IT and OT were built on different assumptions. OT systems were designed for safety, stability, and decades-long lifecycles, whereas IT evolves rapidly, constantly introducing new interfaces, updates, and potential attack surfaces. The mismatch between the two creates exactly the kind of seam that attackers target.

> The only viable path forward is for industries to move from isolated protection to shared protection – building common standards together rather than defending alone.

Healthcare exemplifies the importance of connectivity. The UN aims to connect all hospitals to the internet by 2030[1], but hospitals tend to avoid network connections out of fear of security risks. It is not uncommon to find environments still running outdated operating systems such as XP. This 'isolation' may appear safe, but in fact it is dangerous. When doctors seek convenience and connect unofficially, security holes emerge. Taking a direct approach to digital transformation and having experts design hospital security is far safer and more efficient. If medical data is properly shared, AI-driven diagnostics and pharmaceutical research will advance, and medical inclusion – a future where healthcare is shared globally – will become a reality.

The challenge at the IT-OT boundary is not unique to aviation or healthcare. Energy systems face the same issue: operational technology that has run safely for decades is now being connected to digital platforms, AI systems, and cloud-based analytics. These systems have become prime targets in recent conflicts, where attacks on power infrastructure highlighted how vulnerable OT can be when it is not designed to interoperate securely with IT. Quite simply, without power, computers and the internet do not work. This is why Japan launched the 'Watt-Bit' public-private initiative[2], bringing together power companies, telecom operators, and data-center providers to create shared standards for how energy infrastructure and digital infrastructure should interoperate. It is a concrete example of how IT and OT can be connected safely – not by isolating systems, but by standardizing the interfaces between them.

There are industries that remain wary of connecting to the internet. Power generation, for example, maintains isolated segments to protect its core systems from cyberattacks and accidents. However, with AI utilization in view, it cannot remain disconnected from external networks forever. So, what's the solution? The only viable path forward is for industries to move from isolated protection to shared protection – building common standards together rather than defending alone.

Standardization: A critical management issue and key to connection

Standardization means sharing common elements and creating rules – not regulations, but mechanisms for interoperability. Without agreed formats and quality standards, technologies cannot connect or serve society.

Data quality is critical. Granularity determines reliability. In my research on medical device standardization, precise timestamps of operating-room events are vital for safety and accident analysis[3]. Such standards enable AI to deliver high-quality decisions. When these timestamps and event definitions are standardized, AI can verify what happened, identify deviations, and support safer operations. Standardization gives AI the reliable foundation it needs to make trustworthy decisions and

domain-specific data turns AI from a generalist into a trusted expert. With high-fidelity, domain-specific data, AI performs exceptionally well.

This is especially true in critical infrastructure, where systems like power generation and electricity distribution depend on precise, expert-level understanding. Decades of operational knowledge are now digitized, creating advanced intelligence for sustainable power systems. When this expertise is digitized and standardized, it becomes 'energy intelligence' that allows AI to operate as a true specialist. And further, challenges like decarbonization and AI-driven optimization demand industry-wide collaboration. Standardization facilitates this, connecting power, transport, and supply chains – and unlocking efficiency and new business models.

Standardization has downsides. Excessive uniformity can stifle innovation or lead to monopolies. Yet technology evolves quickly and closed standards rarely endure.

Standardization reshapes cost structures

The greatest value of standardization is its ability to transform cost structures. Shared systems cut Capital Expenditure and Operational Expenditure dramatically, driving down total cost of ownership[4]. This lowers barriers to innovation[5] and lets companies focus on creating value on a common foundation.

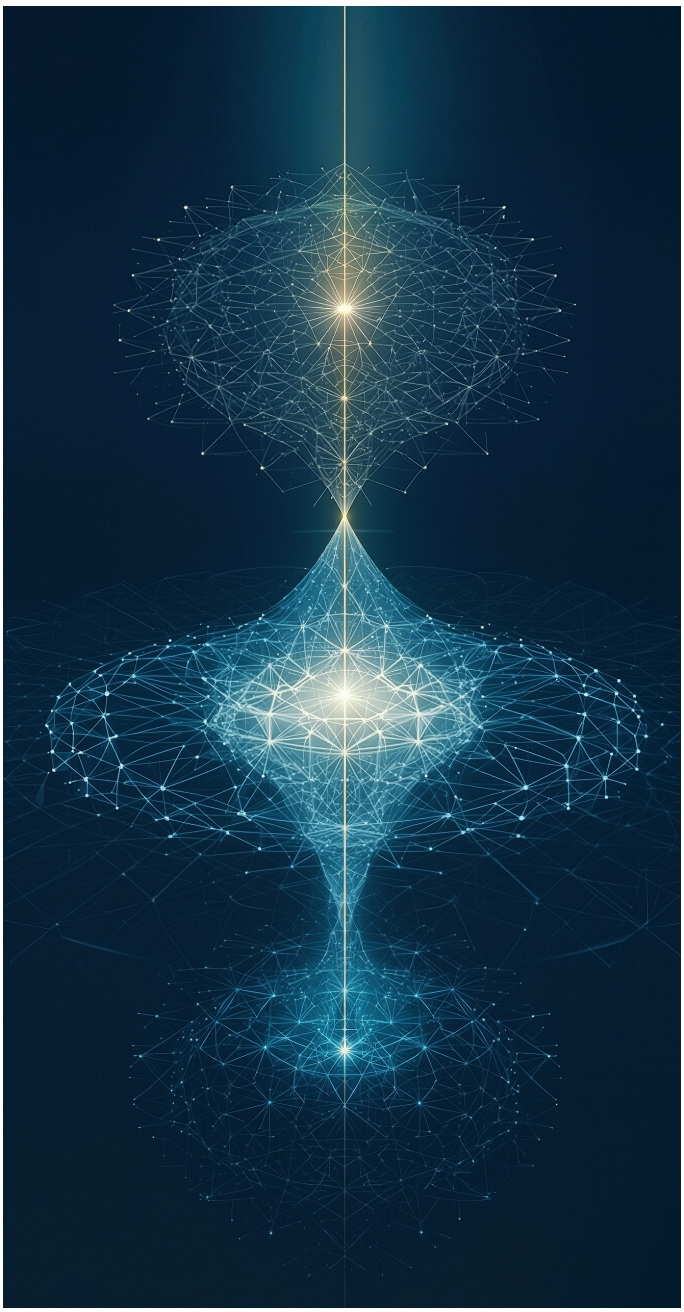
Cloud computing illustrates this perfectly. Built on standardized services and open internet interfaces, it shifted IT from 'ownership' to 'usage'. The National Institute of Standards and Technology's SP800-145 (the US government's definition of the essential characteristics of cloud computing) clarified what 'cloud' actually means, and its adoption has optimized OpEx and fueled a surge in startups.

Before the internet, reaching one million customers required massive investment – dealer networks, factories, logistics. Today, a service created by a teenager can scale to millions with near-zero CapEx and OpEx. Scale is no longer about capital – it's about intelligence and design. Maintaining legacy systems often costs more than innovating.

Cybersecurity is one of the clearest examples of why standardization reshapes cost structures. Maintaining isolated, bespoke security systems is far more expensive – and far less effective – than building on shared, interoperable technologies. To move

toward safety, organizations need common security technologies, common protocols, and the ability to share information quickly when incidents occur. Standardization creates both: interoperability that strengthens collective defense, and a predictable cost structure that reduces the burden on individual companies. In cybersecurity, 'going it alone' is the costliest option.

And when every company is reinventing the same security wheel, costs multiply and resilience weakens. Standardization is not just technical – it's a strategic management imperative.



The CISO's new role and the importance of 'good' use

The burden on security personnel, meanwhile, has grown significantly. CISOs once only handled cyberattacks and fraud, but now service quality, ethics, and even human lives depend on them. Business responsibility increasingly falls on CISOs. In future corporate management, security and IT experts like CIOs and CISOs may need to be placed at the core of management, exercising authority and receiving compensation equal to CEOs – or CEOs themselves may need deep expertise in cybersecurity and risk management.

Additionally, cybersecurity must combine technical and legal defenses with promoting 'good' – that is to say virtual and ethical use. While cybersecurity can block threats through technology and law, expanding 'good' use reduces the space in which abuse can occur. When responsible practices become the norm, misuse is pushed to the margins. Japan's culture of quality and safety shows how 'good' use can be cultivated: a commitment to doing things properly, ethically, and with care for others.

Greater connection leads to greater resilience

Resilience means recovering when something happens and its foundation is connectivity. The internet's complex connectivity allows rerouting when links fail. In disaster-prone Japan – where earthquakes, typhoons, and torrential rains are common – we have accumulated knowledge on how to handle the deceased, identify disaster victims who require constant medication, and deliver pharmaceuticals to them. We have gradually learned where and what is needed, and as a result, many more lives have been saved. However, when critical infrastructure is interconnected, if there is no mechanism for others to compensate, society can come to a standstill. Interconnected systems only create resilience when there are shared standards that allow one operator to compensate for another. Without them, interdependence becomes fragile.

Resilience is not just risk response; it is the core of growth strategy.

Fragility became visible during the Noto earthquake in Ishikawa, when municipal systems lost critical records about residents. What would have happened if Tokyo could have instead reissued essential certificates for displaced people? In a country where major earthquakes are a certainty, cross-regional data sharing should be allowed – Tokyo backed up by Kyushu, or even Tokyo and Sydney backing up each other. For non-sensitive information, even medical records should be exchangeable across regions. And if Japan could maintain sovereign control of its data while hosting a secure backup in places like Australia, hospitals around the world could access essential records when a Japan citizen falls ill abroad. Without such mechanisms, interdependence collapses at the very moment resilience is needed.

Resilience is not just risk response; it is the core of growth strategy. And most importantly, in the post-internet era, leaders must recognize that even if their business scope is limited and their mission appears local, they should actively consider the global significance, implications, and responsibilities their actions have on people around the world.

References

1 United Nations - Achieving universal connectivity by 2030

2 Watt-Bit Public-Private Council (METI)

3 Goldman, J. M. (2011) *Medical Device Interoperability: The Case for a Medical Device Data Language*

4 Carl Shapiro & Hal R. Varian (1999) *Information Rules: A Strategic Guide to The Network Economy*, Harvard Business Press

5 OECD (2016) *The Economic and Social Benefits of Internet Openness*