Nemko Digital



Digital Trust Requirements for Real Estate in Germany:

From inspection excellence to digitally resilient buildings

When strong inspection regimes meet digital reality

Germany's real estate sector is built on a long tradition of rigorous inspection and safety assurance. Mandatory inspections, strict qualification requirements, and close alignment with insurance conditions have created a high level of confidence in the physical safety of buildings. These inspection regimes are not being questioned. On the contrary, they remain the foundation on which trust in the built environment is built.

What is changing is the environment in which these inspections operate. Buildings are no longer composed of largely independent technical installations. They are becoming integrated, software-driven systems whose behaviour depends on data flows, connectivity, and continuous configuration.

Real estate owners and operators already expect systems to function safely and reliably at all times, not only at the moment of inspection. Digitalisation does not change that expectation. What it does change is the level of complexity. As systems become interconnected and remotely managed, ensuring continuous correct behaviour becomes more challenging and involves more parties, technologies, and dependencies.

Digital Trust should therefore be understood as an addition to Germany's strong inspection culture. It builds on existing safety assurance and extends it into the digital domain, where reliability is shaped not only by installation quality, but also by software, data, and integration over time.



Buildings are becoming digital ecosystems

Modern buildings are evolving into digital ecosystems. In many new and renovated buildings, safety, security, and operational systems are already integrated through central software platforms.



Fire alarm systems are designed to automatically trigger door releases, elevator recalls, and ventilation control. Elevators are connected to remote diagnostic and predictive maintenance platforms operated by manufacturers or specialised service providers. Heating, cooling, and ventilation systems increasingly adapt dynamically based on sensor data, occupancy patterns, and, in some cases, external inputs such as energy pricing or grid signals. Large real estate portfolios are monitored from central control rooms, sometimes spanning multiple regions or countries.

These developments are becoming standard in modern commercial, industrial, and public buildings. They improve efficiency, sustainability, and response times. At the same time, they mean that the behaviour of a building increasingly depends on software logic, data quality, connectivity, and ongoing configuration, not only on the physical condition of individual components.

Trust in buildings is therefore no longer limited to the question of whether systems are correctly installed and periodically verified. It also includes whether digital systems interact as intended, remain resilient over time, and respond predictably under changing conditions.

The inspection system remains the foundation, while new risk dimensions emerge

Germany's inspection framework remains the indispensable foundation of building safety. Safety-critical installations are subject to clearly defined inspection cycles, often complemented by additional requirements arising from insurance conditions and building-specific risk profiles. Inspectors are personally recognised and qualified, ensuring a high level of professionalism and independence.

These inspections are essential and will remain so. They confirm that systems are properly installed and function correctly at the time of inspection. What they are not designed to fully address are the digital dependencies that increasingly surround these systems before and after the inspection.

Software updates can alter system behaviour. Remote access arrangements can change. Interfaces between systems can be modified or extended. Data inputs used for automation and optimisation can evolve over time. None of this reduces the value of inspections, but it introduces additional dimensions of risk that sit alongside the traditional physical safety perspective.

As a result, responsibility is no longer confined to a single moment or actor. It is shared across owners, operators, facility managers, and technology providers, and it extends across the entire lifecycle of digital building systems.

Digital Trust regulation and expectations are expanding

Alongside technological change, expectations around digital trust are increasing. A growing set of EU-level digital regulations affects building technologies, often indirectly but increasingly in practice.

The Cyber Resilience Act introduces lifecycle-based cybersecurity requirements for digital products,

including many components used in building systems. Vulnerabilities in these products can directly affect the safety and availability of building operations.

The EU Data Act strengthens rules around access to and use of data generated by connected products. In a real estate context, this applies to data from elevators, energy systems, sensors, and building management platforms. Owners and operators must understand who can access which data, how it may be shared, and how this aligns with contractual and operational responsibilities.

The AI Act becomes relevant where analytics or AI are used in building contexts, for example for predictive maintenance, anomaly detection, access management, or decision support in safety-related processes. Requirements around transparency, risk management, and human oversight increasingly shape how such systems must be governed.

The GDPR continues to apply wherever personal data is involved, including access control, video surveillance, and occupancy analytics. Compliance is not only a legal matter, but also a design and governance issue within modern buildings.

Lastly, the NIS2 Directive is particularly relevant for buildings that host or support essential or important services, such as healthcare facilities, data centres, transport infrastructure, and energy systems. While the regulation applies to the organisations operating these services rather than the building itself, building systems such as access control, building management platforms, and connected infrastructure increasingly fall within the cybersecurity risk and supply chain scope of NIS2-regulated entities. As a result, building owners and operators are increasingly required to demonstrate appropriate cybersecurity governance, resilience, and incident management capabilities to meet tenant, operator, and contractual requirements.

Beyond these examples, further regulatory and contractual expectations continue to emerge through insurance requirements, public procurement rules, and sector-specific obligations. Taken together, they steadily raise the bar for digital control and accountability in real estate, even where owners or operators are not directly in scope of every regulation.

What this means for owners and operators, and why acting now matters

These developments are already visible across Germany and Europe. Fire safety systems are tightly integrated with access control and evacuation logic. Elevators are monitored remotely, with maintenance decisions increasingly driven by data rather than fixed schedules. Energy and ventilation systems are continuously optimised to balance comfort, efficiency, and sustainability. Logistics and industrial facilities rely on digital monitoring to protect sensitive goods and processes. Large property portfolios use centralised platforms to oversee safety, security, and performance across many sites.

In some buildings, early forms of analytics and AI are already used to detect faults, predict failures, or improve operational efficiency. These use cases deliver clear value, but they also increase dependence on digital correctness and structured governance.

For owners, operators, and facility management organisations, the scope of responsibility is expanding. Physical safety remains non-negotiable. At the same time, digital system integrity now directly influences safety, availability, reputation, and insurability.

Disruptions do not have to result from cyber attacks to be significant. Configuration errors, unclear responsibilities, or poorly managed updates can have immediate operational or safety consequences. As systems become more integrated, the causes of incidents become harder to trace and accountability more complex.

Acting now matters because digital complexity accumulates over time. Every retrofit, new service contract, or system integration adds another layer. Organisations that start early can build clarity and governance step by step, rather than reacting under pressure after an incident or during insurance, audit, or regulatory reviews.



Extending inspection excellence through integrated Digital Trust governance

The objective is not to change or diminish inspections. It is to consciously extend assurance beyond the physical safety lens to include digital behaviour and dependencies.

Leading real estate organisations are building on existing inspection excellence by introducing an integrated Digital Trust governance layer. This typically starts with transparency: understanding which systems are connected, how they interact, and which parties are involved. From there, physical and digital risks are assessed together, with a focus on safety-critical and public buildings.

Regulatory, insurance, and contractual expectations are mapped in a structured way. Responsibilities between owners, operators, facility managers, and suppliers are clarified. Digital controls are aligned with recognised standards and governance frameworks to ensure consistency across portfolios and over time.

Importantly, this is not treated as an IT exercise. Inspectors, service providers, and operational teams are part of the same conversation. Digital Trust becomes an extension of building safety and operational governance, not a parallel discipline.



Practical, no-regret steps starting today

For most real estate organisations, the way forward is evolutionary rather than disruptive. Practical steps can be taken today without undermining existing processes.

Start by creating visibility over connected building systems and their dependencies. Prioritise safety-critical installations and large or public buildings. Extend existing inspection logic with questions around software updates, remote access, and data use. Align expectations early with insurers, operators, and key suppliers. Treat Digital Trust as a capability that matures over time, rather than a one-off compliance exercise.

Germany's inspection system provides a strong and trusted foundation. By extending it with Digital Trust governance, real estate owners and operators can ensure that this foundation remains effective in an increasingly digital built environment, preserving safety, reliability, and trust for the years ahead.

About the authors



Bas Overtoom

Bas Overtoom is the Global Business Development Director where he leads global efforts to promote responsible AI adoption at Nemko Digital, working with organizations to operationalize trust, transparency, and compliance in their AI systems. With a strong background in business-IT transformation and AI governance, he brings a pragmatic approach to building AI readiness across sectors.



Jahn Stephansen

Jahn Stephansen, a high-voltage Electrical Engineer graduated from Østfold Engineering School in Norway brings over 30 years of experience in the TIC industry. He started his career as a Test Engineer and lead entire teams as a Lab Manager. For many years, he has also been a Lead Auditor for management system certification. Since 2008, Jahn has been steering Nemko Germany as General Manager

Nemko Digital