Msafe

# The new reality of compliance

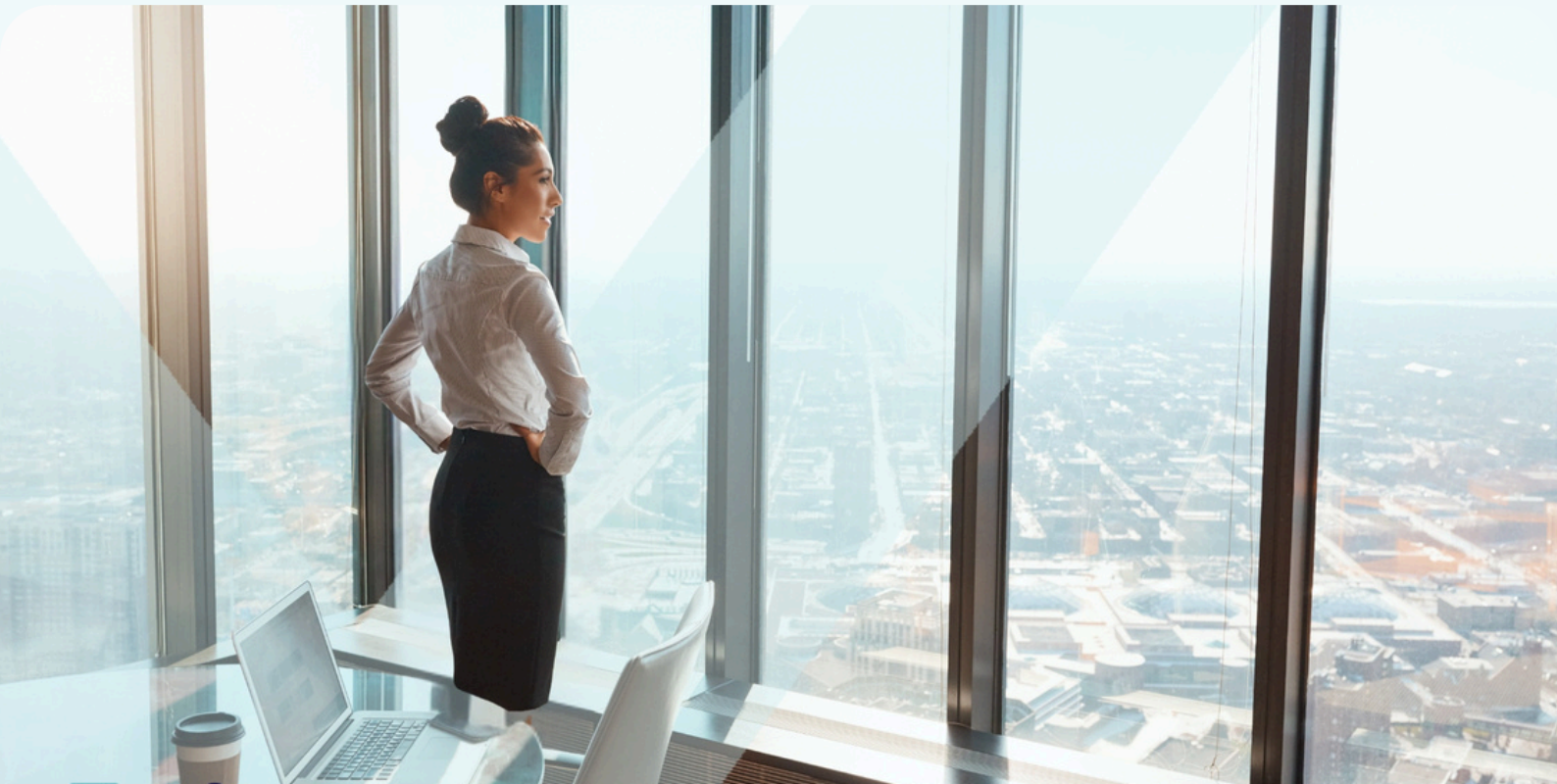
How organisations will remain demonstrably reliable in 2026

# The question is no longer: ‘Are we compliant?’

In 2026, compliance will no longer be a matter for lawyers or auditors. It will have become a management issue, an essential part of good corporate governance.

Under the influence of legislation such as NIS2, DORA and the AI Act, organisations will be expected not only to demonstrate that they comply with the rules, but also that they are structurally organised to do so.

For sectors such as energy, manufacturing and critical infrastructure, this is a fundamental shift.
The question is no longer: *‘Are we compliant?’*
But: *‘Can we prove it — every single day?’*



# From policy to system

Whereas compliance used to revolve around policy, procedures and checklists, the emphasis is now shifting towards building a self-sustaining system. A system in which governance, technology and behaviour are inextricably linked.

In many organisations, this is still a work in progress.
Policies are often well described, but information flows through countless systems and departments. Data is shared, edited and stored without it always being clear where it ends up.

And that is precisely where the risks arise.

"***The biggest risk is rarely in the IT infrastructure" says Thijs van der Linden, COO at Msafe. "It's in something as mundane as sending a file."***

Compliance has thus become not only a technical issue, but above all an operational one.

# A layered approach to control and trust

Organisations that can demonstrate their compliance almost always work with a layered architecture.
No single tool or department can do it alone; it is the cohesion that makes the difference.

# First layer: governance and risk management

The foundation lies in a solid governance and risk framework. Large companies use integrated **GRC platforms** (Governance, Risk & Compliance) such as Workiva or MetricStream for this purpose.

These systems bring together policy, audits, risks and controls in a single environment, creating clarity and predictability.

# Second layer: secure collaboration

However, the greatest vulnerability rarely lies in policy, but in day-to-day collaboration. Many data breaches still occur when sharing files via email, public clouds or temporary platforms.

This is where technology such as Msafe Secure File Transfer comes into play. Msafe encrypts every shared file, keeps track of who shares what and when, and ensures that all data remains within European borders. This eliminates one of the most underestimated risks: routine human actions that take place out of sight.

# Third layer: privacy and supplier management

No organisation operates in isolation anymore. Suppliers, service providers and partners are all part of the same digital chain. Tools such as OneTrust and Centraleyes provide insight into who has access, what data is processed and where responsibilities lie.

Together, these three layers form a structure in which compliance is **no longer checked retrospectively, but is ingrained in daily practice.**

# Integration instead of fragmentation

The real challenge lies not in choosing the tools, but in how they work together. Without integration, compliance remains fragmented: an audit here, a policy there, a report in Excel.

Mature organisations connect their systems to each other. The audit logs from Msafe automatically flow to the GRC dashboard. Privacy assessments are linked to project management. And deviations in access management lead to automatic notifications in the risk framework.

The result is a continuous, **dynamic picture of compliance**, rather than isolated snapshots.

# The value of demonstrability

***What does this deliver in concrete terms?***
First and foremost, **peace of mind** and **predictability**.
Audits are completed more quickly because **evidence is immediately available**.
Incidents are **detected sooner**.
And the organisation **does not have to wait for external audits** to know where it stands.

**Compliance thus changes from an obligation to a tool: a way to keep control of processes and risks.**

Managers in the industrial sector are increasingly using one word to describe what it's all about: demonstrable compliance. Those who can show that they are in control not only gain time, but also the trust of customers, regulators and employees.

# The human dimension

Technology provides the structure, but people give it meaning.
A mature compliance culture only emerges when employees understand why compliance is important. This requires clarity, simplicity and repetition.

Complex processes invite detours.
Simple processes are followed automatically.
That is why more and more organisations are investing in tools that **make compliance invisible** and self-evident, such as Msafe.

By making secure file transfer as easy as email, compliance is no longer an extra step, but a natural reflex.

# From control to culture

The development of compliance reflects a broader movement within organisations: from control to culture, from obligation to conviction.

Those who make this transition now are building something that cannot be copied: **credibility**. Because in a market where almost every supplier claims to be compliant, the ability to **prove** it is what sets them apart.

And that is precisely what the future of compliance is all about. Not ticking boxes, but building trust.

# Want to know more?

**Would you like to know how Msafe fits into your organisation's compliance architecture?**

Contact us for a no-obligation consultation about secure and demonstrable file transfer within your governance structure.

Linnaeusweg 9a | IJsselstein
The Netherlands
+31 88 88 53 010
info@msafe.co
msafe.co