








Myth vs. Reality: ISO 27001 Automation

"Platforms automate ISO 27001, so we don't need consultants."  Platforms automate technical checks, not risk management, governance, or compliance strategy.

 "Most ISO controls are automatable."  Only ~7–10 controls (out of 93) are fully automatable. The rest need policy, people, or process alignment.

 "Automated deletion and masking remove manual work."  Execution can be automated, but humans must define rules, align to law, and approve exceptions.

 "Dashboards show we're compliant."  Dashboards show status of configurations—not whether your controls are fit-for-purpose or legally compliant.

 "Automated alerts equal faster incident response."  Tools may detect events—but only humans can triage, escalate, report to authorities, and align with GDPR, DORA, AI Act.

 **Key Takeaway:** *"Automation is your assistant—not your strategist. ISO 27001 success comes from combining smart tools with smarter people."*

Capabilities Comparison: Compliance Platform vs. ISO 27001 Consultant

Capability Area	Compliance Platform (e.g., Vanta, Drata)	ISO 27001 Consultant
Evidence Gathering	✔ Automated from cloud tools (AWS, Okta, etc.)	✦ Manual or guided collection
Control Monitoring	✔ Continuous checks for misconfigurations	✘ Relies on external tools or client reporting
Risk Assessment	✦ Basic asset/control visibility	✔ Full risk methodology, likelihood/impact analysis, risk appetite mapping
Policy Development	✘ Templates only	✔ Tailored, operationally embedded, regulator-aligned
Process Design (e.g., JML, backup, change)	✘ Not provided	✔ Designs business-aligned, auditable processes
Incident Response Alignment (GDPR, DORA, CRA, AI Act)	✘ Not covered	✔ Maps escalation flows, competent authorities, and statutory timelines
Role & Responsibility Clarity	✘ Not defined	✔ Maps stakeholders, builds RACI, trains teams
Stakeholder Training	✘ Not included	✔ Provides awareness programs, exec briefings
BAU Integration	✘ Dashboards only	✔ Aligns controls with operations, KPIs, audits
Audit Support	✔ Evidence export, control mapping	✔ Pre-audit readiness, coaching, gap closure
Board Reporting	✦ Tech dashboards (e.g., % MFA use)	✔ Risk-level insights, trend reporting, strategy mapping
Supplier & Regulator Engagement	✘ Not supported	✔ Aligns supplier contracts, identifies regulatory contact points
Post-Certification Support	✦ Platform maintains continuous monitoring	✔ Supports internal audits, maturity roadmap, recertification strategy

Final Summary

Use automation platforms

To gain speed and visibility.

Use consultants

To gain strategic clarity, policy alignment, and regulatory assurance.

Together, they transform ISO 27001 from a checkbox exercise into a **business enabler**.

www.iso27k.co.uk info@iso27k.co.uk © 2025. All rights reserved.

