Digital Sovereignty as a Growth Accelerator

KWCON 2026

November 9, 2026

Andreas Stemick





Andreas Stemick

A pioneer for digital sovereignty in Europe

> **“Technology is rarely the bottleneck. It’s the ability to create options and actively manage risks.”**

Managing Partner

BDO DIGITAL & BDO Cyber Security

Equity Partner

AG Wirtschaftsprüfungsgesellschaft

Advisory Leadership

Member of the Advisory Leadership Team at BDO AG WPG

Digital Sovereignty Program

Helping pave the way for the DSP in Europe

© BDO

The journey in 5 steps

Agenda

01

The reality of the cloud

Mainstream meets concentration

02

The kill-switch risk

Average survival time: 11–12 months

03

AI changes the rules

Automated exploits add a new dimension

04

Sovereignty: How?

Three levels of action, one goal

05

The way forward

BDO & kwsoft® as anchors

© BDO

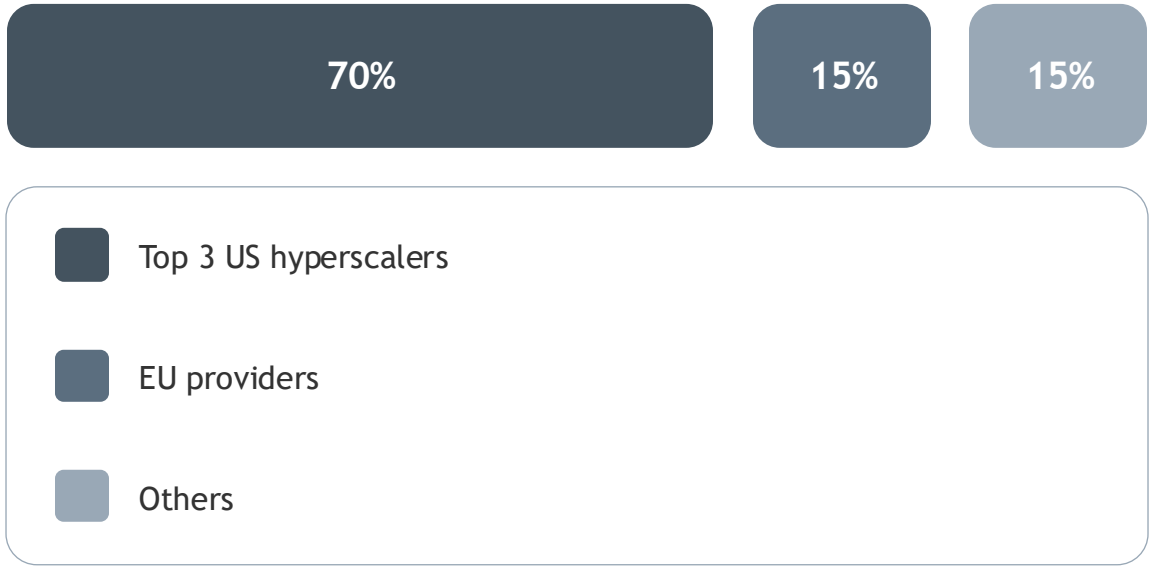
Cloud is mainstream — and a dependency

The cloud reality

52.74%

of EU companies use paid cloud services
+7.42 percentage points compared with 2023
84.67% among large enterprises

Market share of cloud infrastructure in Europe (2024)



€61 billion cloud market —
Value creation flows out.

Sources: Eurostat, ICT survey 2025 · Synergy Research Group (market shares, 2024)

© BDO

One year until the lights go out

The “kill switch” risk

How long can your company survive if digital services can no longer be sourced from abroad?

Abroad (overall)

57%

Survive up to 12 months

USA

Ø 12

Months of survival

China

Ø 11

Months of survival

Only 4% of companies could permanently manage without importing digital technologies from abroad.

Source: Bitkom Research, Nov. 2025 (605 companies with 20 or more employees) · Based on: Companies that import digital technologies

© BDO

Five factors highlighting the urgency

Cloud sovereignty · Need for action

Awareness is growing — but the ability to act is not. Five facts highlighting the need for action in Germany and Europe.



Market concentration

The top three U.S. providers account for around 70% of the European market.



Critical infrastructure & public sector

Risks are high for public authorities and critical infrastructure without a European cloud.



Regulatory conflict

U.S. CLOUD Act vs. GDPR — structurally incompatible.



EU initiatives

GAIA-X and the government cloud have been launched — impact remains limited so far.



Strategic risk

Dependence on the U.S. acts as a “kill switch” and creates geopolitical leverage.



Europe’s window of opportunity is closing.
Put structures in place now — don’t just react.

© BDO

Sovereignty means

having a controlled exit from the kill switch.

Not a panic-driven emergency shutdown – a controlled, tested, auditable exit.

What works for your environment?

© BDO

Interim assessment

Awareness is growing — but the ability to act is not.

Europe’s window of opportunity is closing. Put structures in place now — don’t just react.

Andreas Stemick · BDO

© BDO

When AI writes exploits itself

The new dimension

Claude Mythos Preview (April 2026) autonomously identified more than 10,000 critical vulnerabilities in its first month. Since June, the Mythos-class model has been publicly available as “Fable,” with restrictions on cyber requests.

Before		Now	
1990s	Automated search for known vulnerabilities	**2026**	AI finds unknown vulnerabilities AND autonomously develops exploits
2000s	Automated search for unknown vulnerabilities	**Scalable**	More than 10,000 vulnerabilities in one month — at industrial scale
Manual	Exploitation and exploit development by humans	**0-day by AI**	Political and technical control become existential issues

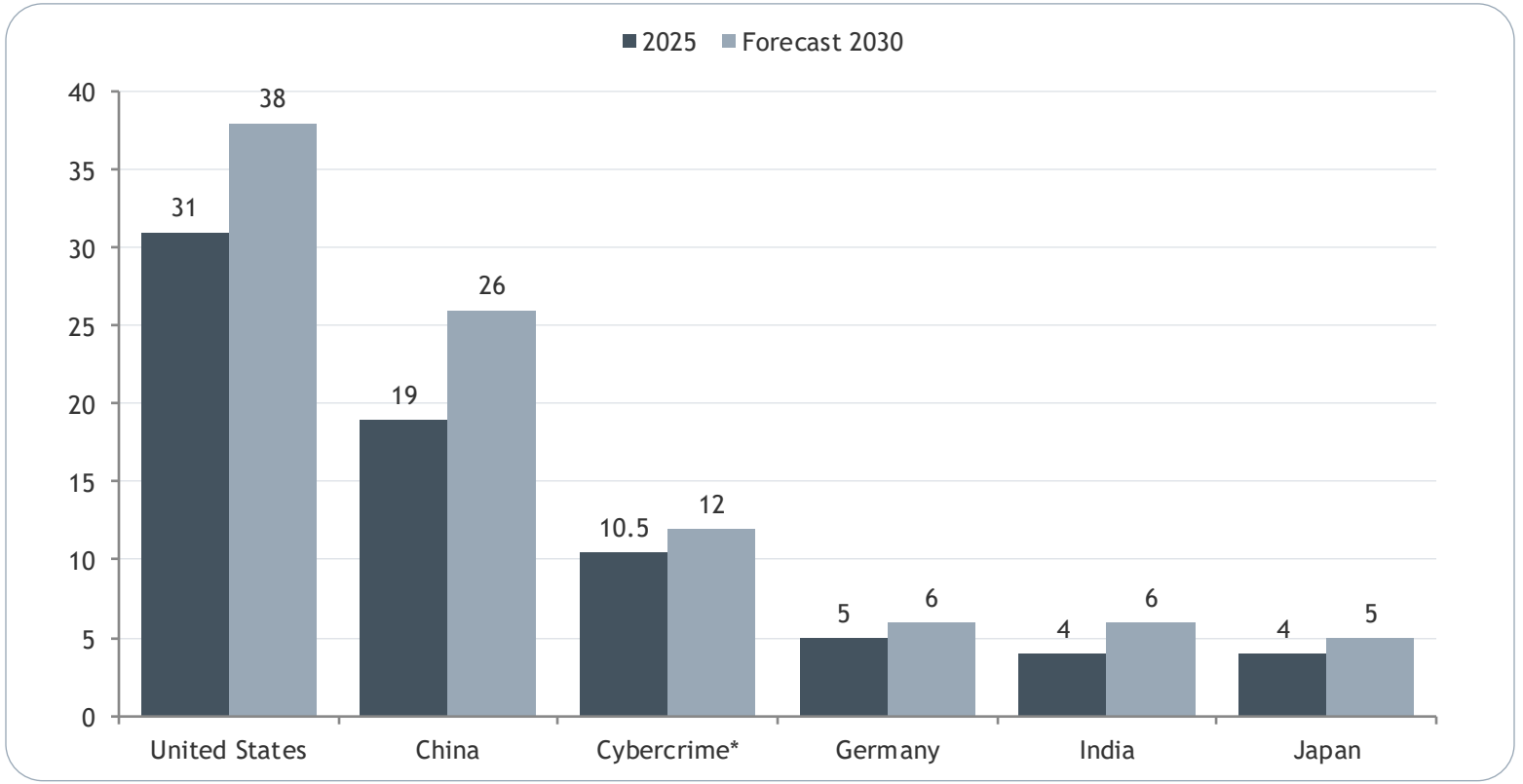
Strategic implication: Stop thinking in terms of services – think in terms of capabilities.

© BDO

Cybercrime as the world’s third-largest economy

The economics of risk

Estimated global cost of cybercrime compared with the nominal GDP of leading economies (in US$ trillions)



Cybercrime

12

Trillion US dollars by 2031

Already around US$10.5 trillion in 2025 — more than three times the 2015 figure (US$3 trillion).

Sources: IMF World Economic Outlook (April 2026); Cybersecurity Ventures, Cybersecurity Almanac (Dec. 2025). *Cybercrime: Forecast for 2031.

© BDO

When devices become attack surfaces

Current incidents · October 2026

Two incidents from the same week: attackers take over connected systems while they are operating – or tamper with devices before they reach customers.

Connected systems · France

50 °C

In the freezers of hundreds of supermarkets

Hackers manipulated connected refrigeration controls (Danfoss) overnight at Intermarché, Coopérative U, Carrefour, and other retailers, forcing defrost mode and setting the target temperature to 50 °C.

Consequences: Spoiled goods and millions in damages. According to the manufacturer, the systems were running outdated firmware.

Supply chain · Hardware wallets

93 million

US dollars stolen from more than 300 wallets

Tampered Ledger Nano X devices appeared in retail channels in Asia and Europe. An additional chip reads the seed phrase from the display, while an LTE modem and eSIM transmit it to the attackers.

Not a factory issue: The devices were intercepted and modified in the supply chain.

If you don't control the firmware and the supply chain, you don't control your devices.

Sources: Reuters, AFP, Franceinfo via ORF, and Berliner Zeitung (October 13, 2026) · heise online, Tom's Hardware, Tibane Labs (October 2026)

© BDO

Three levels. One goal.

How sovereignty is achieved

Complete sovereignty is unrealistic. The goal is risk-proportionate sovereignty – across three levels of action.

01 **Technical**
Infrastructure & architecture

- Open-source stack: SCS, OpenStack, Kubernetes
- EU-owned key management — no US KMS
- Confidential computing / TEEs for sensitive workloads

02 **Organizational**
Infrastructure & architecture

- Exit strategy, monitoring, audit rights
- Data classification based on sovereignty requirements
- IR capabilities without reliance on US providers

03 **Industrial policy**
Framework & ecosystem

- Government as an anchor customer for EU providers
- EU Chips Act, fiber optics, skilled workforce
- EUCS with genuine sovereignty requirements

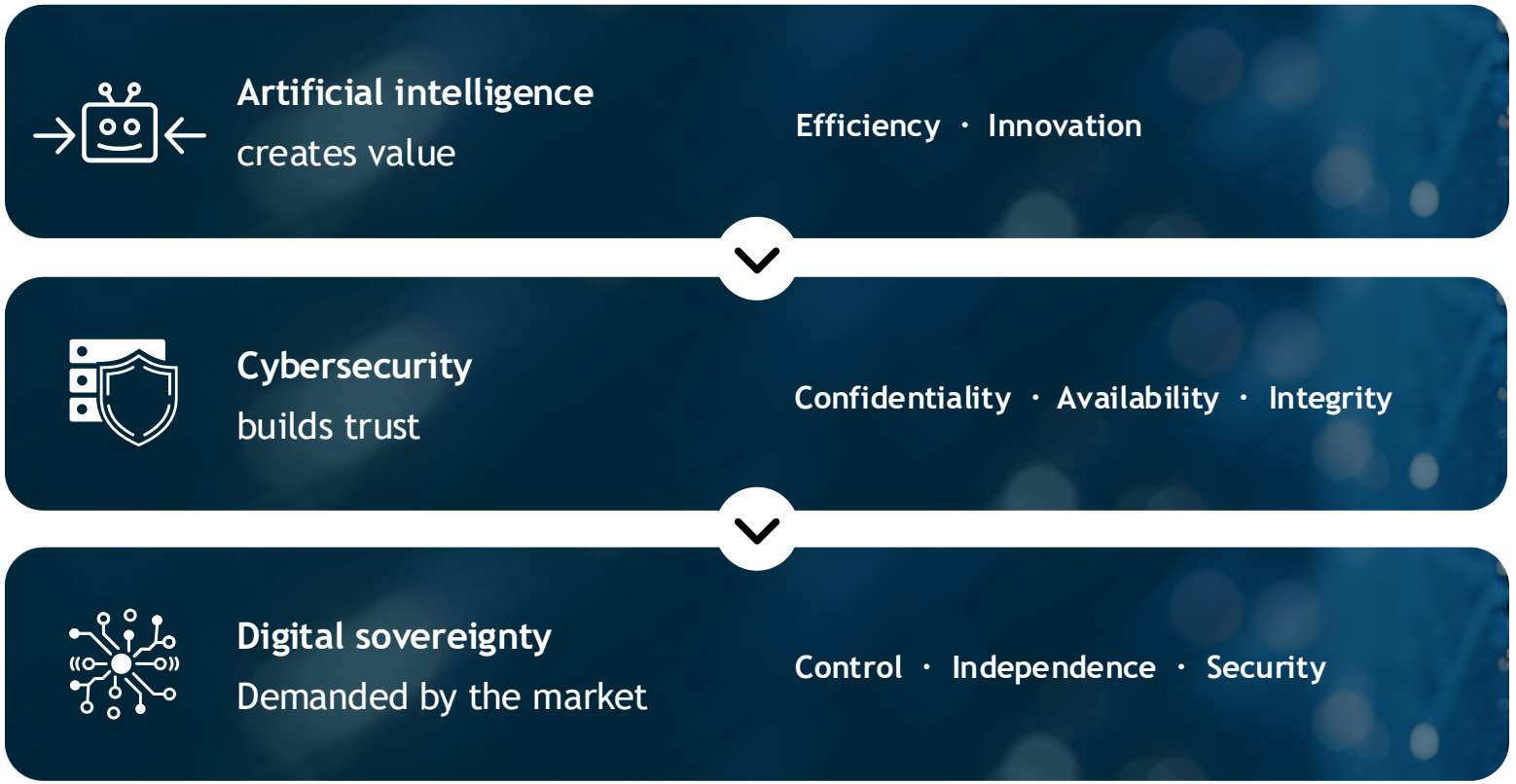
Sovereignty = choice + verifiability. Not ideology – architecture.

© BDO

Bringing AI, cybersecurity, and ISVs together

Sovereignty as a product feature

Sovereignty as a must-have product feature – three layers that build on one another and open up new market opportunities for ISVs.



Opportunities for ISVs

Competitive advantage

"Sovereignty-ready" opens doors to regulated industries.

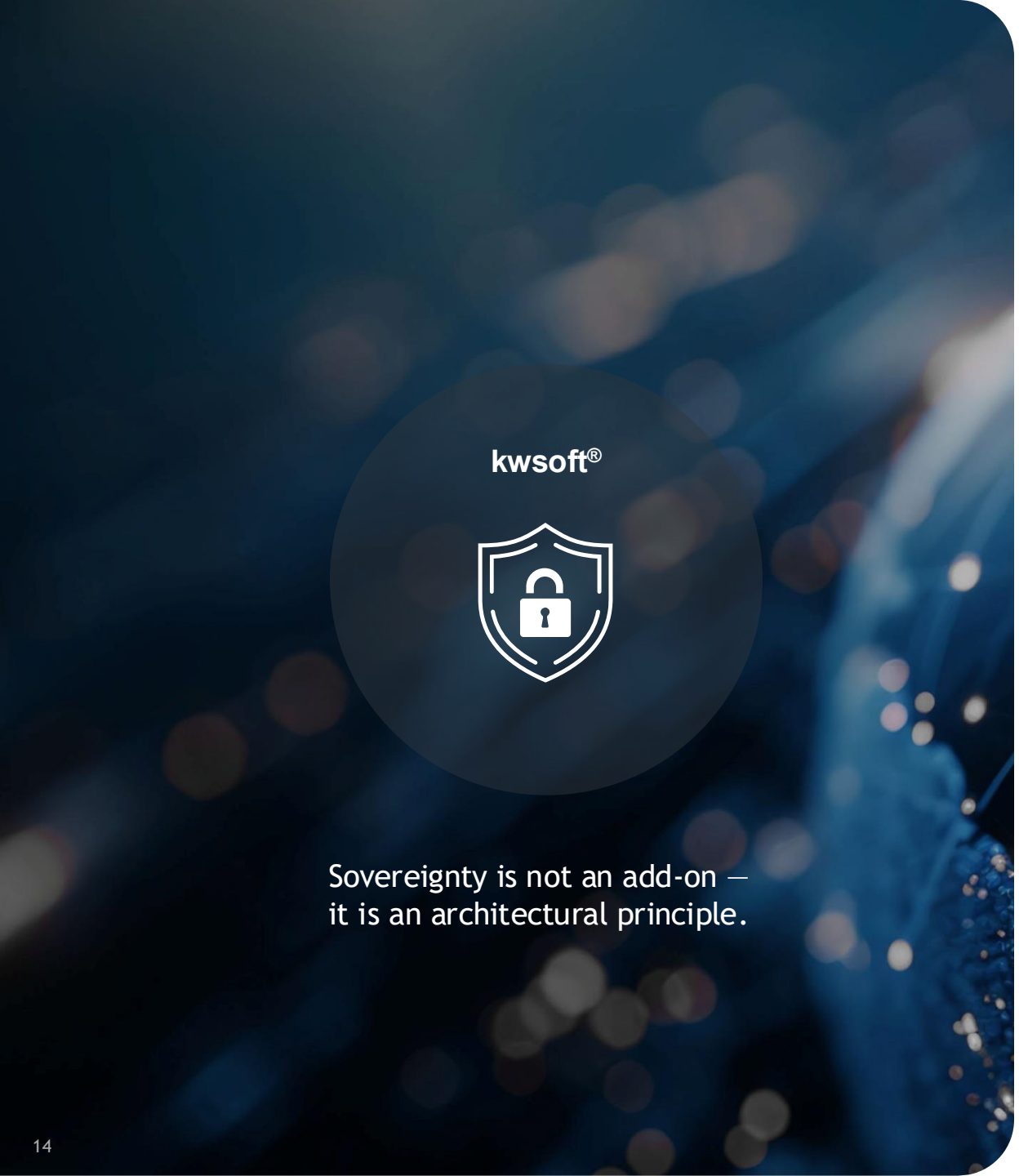
Efficiency

XaaS enables fast, scalable implementations.

Trust

Audit evidence and portability strengthen customer retention.

© BDO



kwsoft® — sovereignty by design

Positioning

Independent

100% owner-operated — no investor pressure, no takeover risk.

Made in Europe

Developed entirely in Germany and the Czech Republic.

AnyPrem and seamless migration

Your data stays in the infrastructure of your choice — GDPR, DORA, banking secrecy.

ISO 27001, EcoVadis, ISO 9001, ISAE 3402

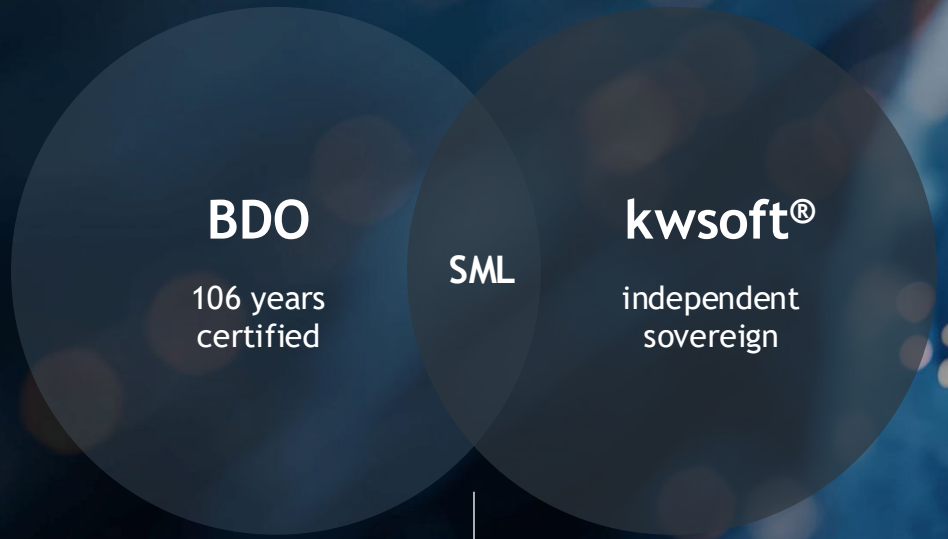
Organizations in the kwsoft® Group meet all relevant certification requirements.

Sovereign AI processing

All AI features can be used with local or privately hosted models.

© BDO

Secure enterprise content cloud services — from certified operations to objective maturity assessment.



Sovereignty Maturity Level
Certified by BDO & StackIT

BDO + kwsoft® — measurable sovereignty

The partnership

Transparent
Objective evidence of the level of digital sovereignty

Regulatory compliance
GDPR · NIS 2 · DORA — reliably documented

Low investment requirements
Fewer hurdles — especially for the public sector and critical infrastructure

Fast
Faster decision-making thanks to clear evidence

© BDO

Five things to remember

Key takeaways

01

Cloud is the standard

The decision to move to the cloud has been made. Governance is the differentiator.

02

Sovereignty = choice + evidence

Organizations need real options – and must be able to audit them.

03

AI makes security mandatory

Automated exploits fundamentally change the risk profile.

04

Stack + operating model

European hyperscaler + kwsoft® + BDO = scalable and auditable.

05

Controlled exit from the kill switch

Not a panic-driven shutdown – but a controlled, auditable exit.

© BDO



BDO AG Wirtschaftsprüfungsgesellschaft, a German company limited by shares, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. © BDO

© BDO