SOR2TIX-AR

ISO 27001:2022 Implementation

Turning Unknown Security Gaps Into Measurable Risk Reduction

Designed for CTOs, CISOs, Compliance Officers, Quality Heads, and Board Members. Gives you a verified view of your real risk posture, not just policy compliance. Helps you prioritize fixes that actually cut breach likelihood, audit exposure, and certification timelines.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

ISO 27001:2022

briskinfosec.com

ISO 27001 Compliance The Gaps Most Organizations Don't See

70% Fewer Security Incidents ISO 27001-certified organizations experience 70% fewer security incidents than non-certified peers. Source : IBM Cost of Data Breach Report. The standard works when it is implemented, not just documented.

What You Think vs What We Find

Common Belief	Reality
We are still on ISO 27001:2013 and our certificate is valid	Certificate holders must transition to ISO 27001:2022 or lose certification.
We purchased a policy template set, so our documentation is covered	Without operational evidence, a policy-only approach fails the Stage 2 audit.
ISO 27001 is built for large enterprises	ISO 27001 scales to any size scope: a single unit or full organization, even under 50 staff.
Certification means we are fully secure	ISO 27001 certifies risk-managed, evidence-based security maturity-not zero incidents.
We can handle the implementation internally	85% of unguided first attempts fail Stage 2, adding 6-12 months. Expert help cuts that.

The Real Cost of Inaction – And Why Prevention Is 30–60x Cheaper

$4.88M
Global Average Cost of a Data Breach
IBM Cost of Data Breach Report record high

144
Countries With Data Privacy Laws
Requiring demonstrable security controls

85%
First-Time Failures
Without expert guidance, miss Stage 2 audit on first attempt

ISO 27001 Implementation Cost

$50,000—$150,000
one-time for a mid-market organization

- Gap analysis and scoping
- Control implementation and evidence collection
- Stage 1 and Stage 2 certification audit

Cost of a Single Breach Without ISMS

$4.88M global average 30–60x the cost of prevention

- Regulatory fines and legal exposure
- Operational downtime and remediation
- Reputational damage and lost procurement

$3.4M Expected Loss Avoidance

Per avoided breach incident. ISO 27001-certified organizations experience 70% fewer incidents than non-certified peers (IBM).

30—40% Cyber Insurance Reduction

Premium reduction for organizations with certified security programs. Insurers increasingly require demonstrated controls, not just declared ones.

40—60% Compliance Spend Reduction

Reduction in parallel compliance spend across GDPR, NIS2, HIPAA, and DPDPA when ISO 27001 serves as the base control framework.

Compliance Fines Avoided

GDPR	Up to €20M or 4% of global annual turnover	Failure to implement technical and organizational security measures (Article 32)
NIS2	Up to €10M or 2% of global turnover	Inadequate risk management and incident handling for essential entities (Art. 21)
DPDPA	Up to ₹250 crore per breach	Data security obligations for data fiduciaries extraterritorial scope
HIPAA	$100—$50,000 per violation, up to $1.9M/year	Lack of documented safeguards and risk analysis for protected health information

Framework Penalty Trigger

ISO 27001:2022

Overcoming Resistance The Hidden Cost of Delay

What Clients Say	Why It Costs More	The Fact
We've never had a breach	Breaches go undetected for an average of 204 days most organizations don't know what they don't know	Average breach cost : USD 4.88M. Long-lifecycle breaches : USD 5.46M
We're behind a firewall	Most database breaches originate from the application tier, bypassing perimeter controls entirely	SQL injection remains in the OWASP Top 10 because it continues to work
We patched recently	Configuration security and patch currency are separate dimensions both must be tested	Default accounts and enabled dangerous features are among the most common assessment findings

What We Test

Active Vulnerabilities in Your Environment

The 2022 revision added 11 new controls specifically because these threat categories were not formally governed in 2013. These are the domains where gaps are most commonly found during Stage 2 audits.

Identity & Access

Privilege escalation, orphaned accounts, and missing MFA across cloud and on-premise environments

Cloud Security (5.23)

Cloud services used without a dedicated security policy, no service inventory, and no risk classification new mandatory control in 2022

Threat Intelligence (5.7)

No formal threat intelligence program feeding into risk assessment a new mandatory control that did not exist in ISO 27001:2013

Data Leakage Prevention (8.12)

Sensitive data exfiltration paths unmonitored across email, endpoints, and cloud storage not formally governed under 2013 standard

Data Masking (8.11)

Production data used in test environments without masking controls a new 2022 control with direct GDPR and DPDPA implications

Secure Coding (8.28)

SDLC without formal secure coding standards new control requiring documented principles and evidence of developer training

Supplier Security (5.19-5.22)

Third-party vendors managed informally, without contractual ISMS requirements or periodic security reviews

Physical Monitoring (7.4)

Physical security monitoring newly required in 2022 organizations without documented perimeter controls and monitoring logs will fail this clause

Did You Know?

57 existing controls were consolidated in the 2022 revision. Organizations on ISO 27001:2013 cannot simply audit against their existing documentation evidence, policies, and the Statement of Applicability all require review.

Every Layer, Every Component

All 93 Annex A controls map to one of four themes. This replaces the 14-clause structure of ISO 27001:2013. Our assessment covers every theme, every control, every layer of your ISMS.

Organizational (37 Controls)

- Policies, roles, and responsibilities review
- Threat intelligence program (5.7) new 2022 control
- Supplier security (5.19-5.22) contractual ISMS requirements
- Cloud service security policy (5.23) new 2022 control
- Incident management and business
- continuity
- Statement of Applicability (SoA) rebuild and validation

Physical (14 Controls)

- Physical security perimeters and access controls
- Equipment maintenance records
- Clear desk and clear screen policy enforcement
- Physical security monitoring (7.4) new 2022 control
- Secure disposal of media and equipment

People (8 Controls)

- Pre-employment screening processes
- Security awareness training evidence
- Disciplinary process documentation
- Remote working policies and controls
- Confidentiality obligations and NDA coverage

Technological (34 Controls)

- Access control and privilege management
- Malware protection and logging
- Encryption and key management
- Configuration management (8.9)
- Data masking (8.11) and DLP (8.12) new 2022 controls
- Secure coding standards (8.28) new 2022 control

We assess EVERY control, EVERY theme, EVERY layer of your ISMS because that is the only way to provide a defensible Statement of Applicability and a Stage 2 audit that holds.

Regulatory Frameworks ISO 27001:2022 Supports

Organizations that achieve ISO 27001 certification create a compliance foundation that satisfies requirements across jurisdictions simultaneously.

GDPR | NIS2 | DPDPA | SOC 2

Where Most Organizations Are Today and Where ISO 27001 Takes Them

ISO 27001 implementation cost for a mid-market organization : $50,000-$150,000 one-time.
Global average cost of a data breach : $4.88M.

Current State (Without ISO 27001:2022 ISMS)

- Security controls documented but not demonstrably operational
- No formal risk assessment methodology tied to Annex A controls
- Supplier security managed informally, without contractual ISMS requirements
- No threat intelligence program in place (new mandatory control 5.7)
- Cloud services used without a dedicated security policy (new control 5.23)
- Data masking and DLP not formally governed (controls 8.11, 8.12)
- Board lacks an evidence-based answer on information security posture

Future State (With ISO 27001:2022 ISMS Certified)

- All 93 Annex A controls assessed, implemented, and evidenced
- Formal risk treatment plan tied to business context and updated annually
- Supplier security reviewed and contractually governed per Annex A 5.19-5.22
- Threat intelligence program operational and feeding into risk assessment
- Cloud security policy in place with service inventory and risk classification
- Data masking, DLP, and secure coding policies operational with audit evidence
- Board receives structured ISMS performance report at management review

What a Certified ISMS Protects and Enables

These figures represent outcomes from organizations that treat ISO 27001 as an operational program, not a documentation exercise.

$3.4M

Expected Loss Avoidance

Per avoided breach incident. ISO 27001-certified organizations experience 70% fewer incidents than non-certified peers (IBM).

30-40%

Cyber Insurance Reduction

Premium reduction for organizations with certified security programs. Insurers increasingly require demonstrated controls, not just declared ones.

60-90 days

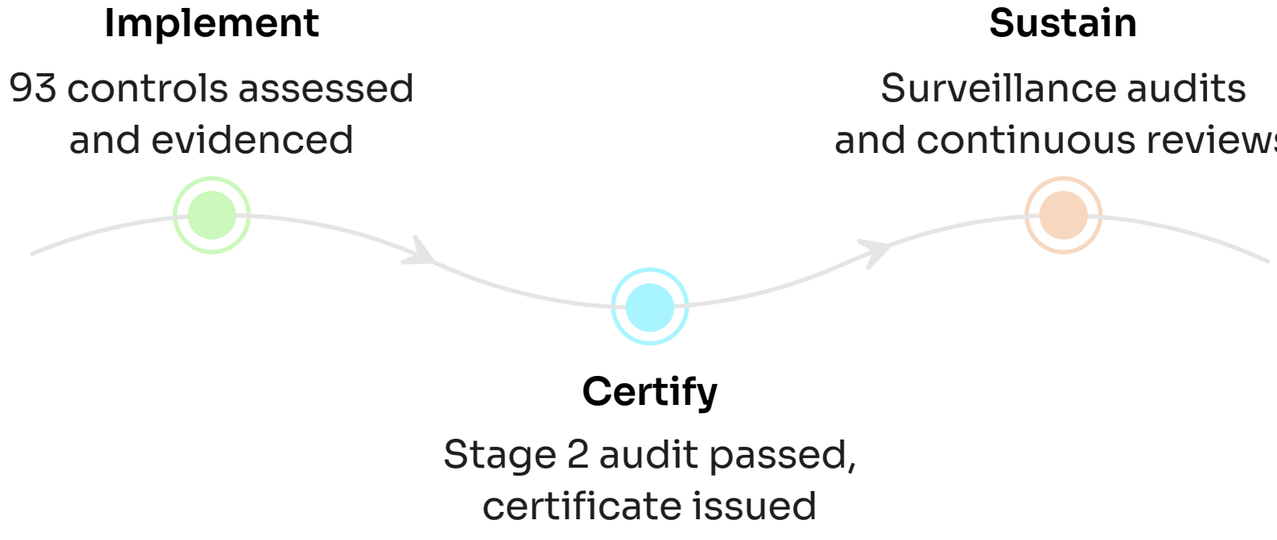
Procurement Delay Removed

Enterprise procurement delay removed. ISO 27001 certification is a prerequisite for UK Government contracts, Singapore GovTech, and large financial institution vendor panels.

40-60%

Compliance Spend Reduction

Reduction in parallel compliance spend across GDPR, NIS2, HIPAA, and DPDPA when ISO 27001 serves as the base control framework.



The pattern across organizations that have successfully transitioned is consistent: the ones that struggled treated 2022 as a documentation exercise. The ones that succeeded treated it as a control effectiveness review.

What the Right ISO 27001 Partner Brings to Your Engagement

The partner you choose shapes how smoothly the transition from gap analysis to certification audit goes.

Capability	Typical Consultancy	BriskInfosec Approach
Accreditation	Self-certified or limited scope	CREST Approved (India's ONLY) + CERT-In + ISO 27001:2022 Certified
bSAFE Framework	Generic gap analysis templates	Proprietary 7-layer, 73-control maturity scoring system, quantified baseline before implementation
SoA Development	Checkbox-based template mapping	Defensible SoA built from your actual risk context, not a boilerplate
New Controls	General guidance on 11 new controls	Implementation support for threat intelligence, cloud security, DLP, and secure coding controls
Compliance Overlap	ISO 27001 in isolation	ISO 27001 mapped to GDPR, NIS2, DPDPA, RBI, SEBI, HIPAA, MAS, and FCA simultaneously
Audit Readiness	Documentation review before audit	LURA portal : AI-powered evidence collection and audit readiness monitoring throughout implementation
Post-Certification	Report and exit	Ongoing surveillance audit support, annual review cycles, and LURA portal for continuous compliance tracking

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited
Internationally certified penetration testing excellence

CERT-IN Empanelled
Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified
Our own security practices are independently audited and verified annually

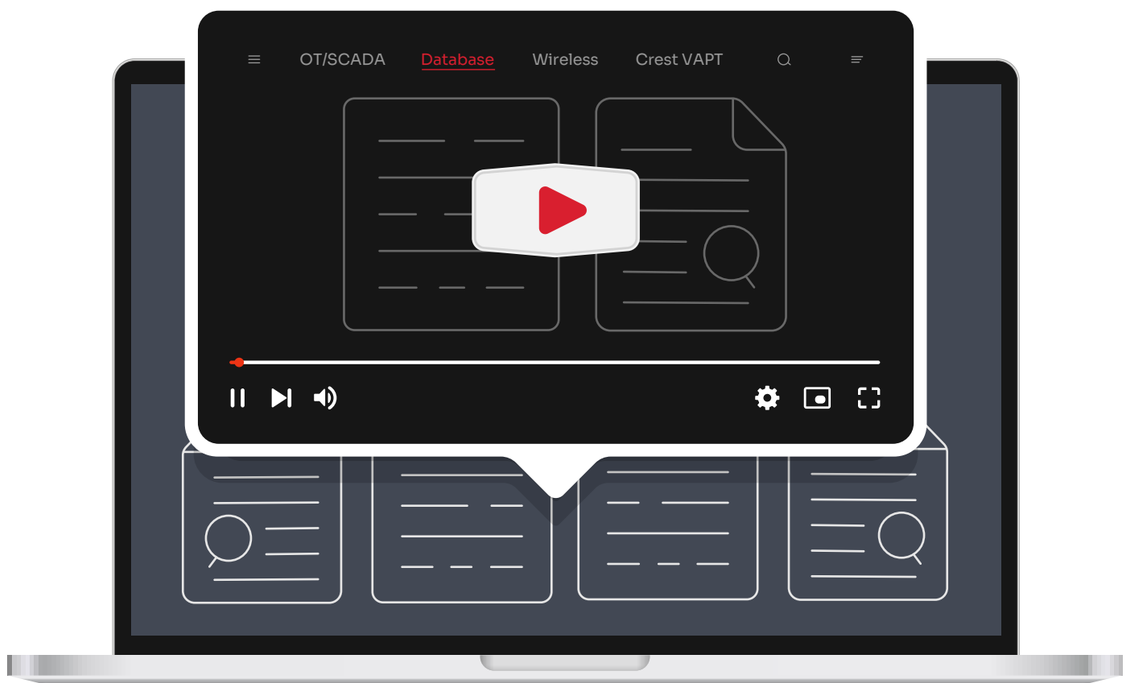
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE
consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence
India
UAE