Third Eye Review Assessment : Independent Validation

A strategic briefing for CISOs, CTOs, audit leaders, and boards. Gain an independent view of your security posture, benchmarked against real-world evidence to uncover hidden gaps.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

TERA

Third Eye Review Assessment

Why Even Strong
Security Programs Benefit From an Outside Perspective

These figures reflect a consistent pattern across thousands of independent security assessments. They are not warnings. They are shared data that helps leadership teams ask better questions.

68%

Organizations That Overestimate Maturity

Organizations that overestimate their own cybersecurity maturity by two or more levels on a five-level scale. Internal teams assess controls using the same assumptions that built them.

258

Days — Average Breach Lifecycle (IBM)

Attackers operate for months inside networks before discovery, internal monitoring often misses what an independent review would surface.

45–75

Security Tools in Enterprise

Average number of security tools deployed. Tool sprawl without independent validation frequently results in misconfigured, redundant, or under-tuned controls.

$4.88M

Global Average Breach Cost (IBM)

Most of this cost traces back to gaps that a pre-incident independent review would have identified.

Key Insight

The pattern that emerges across independent assessments is consistent: organizations with active compliance certifications, dedicated security teams, and meaningful security budgets still carry material blind spots.

This is not a failure of competence. It is a **structural limitation of internal review.** The **Third Eye Review** is designed to address exactly that limitation.

The Landscape Your Peers Are Navigating

Published data shaping how boards and audit committees approach independent security assurance.

15,847+

Vulnerabilities Identified

Not visible to internal teams **(Briskinfosec assessment history)**

$127M

Breach Costs Prevented

Estimated across Briskinfosec client base

30–40%

Insurance Premium Reduction

Cyber insurance premium reduction for orgs with documented security maturity evidence

2–3x

Higher Remediation Cost

When gaps are found at audit time vs. pre-audit review

CREST Accredited certin Empanelled

Five Conversations
We Have With CISOs and Audit Teams Every Week

These are not misconceptions to correct.
They are reasonable assumptions that need updated context.

WHAT YOU THINK	THE REALITY
"We passed our last audit, so our security program is effective." This is a logical position and a common starting point for the conversation.	**Audit certification validates process compliance at a point in time, not resilience against current adversary tactics.** Organizations with active ISO 27001 and PCI DSS certifications are breached regularly. Certifications are backward-looking compliance exercises. A **Third Eye Review** is a forward-looking effectiveness check.
"Our internal team knows our environment better than any outside assessor." That is true for operations. It becomes a limitation in security assessment.	**Internal knowledge of the environment is an operational advantage, not an assessment advantage.** External assessors bring adversarial perspective, global benchmark data, and freedom from the organizational assumptions that internal teams cannot step outside of.
"We have an internal audit function, so an external review is redundant." Internal audit is a valuable control. It covers different ground than a **Third Eye Review.**	**Internal audit validates control existence and documentation.** A Third Eye Review validates control effectiveness against real-world threats, tests controls that internal audit cannot test, and benchmarks maturity against industry peers using data from 4,800+ assessments.
"An external assessment will just confirm what we already know." It might. But the data from our assessment history suggests otherwise.	**Across 4,800+ assessments, Briskinfosec has consistently identified material vulnerabilities and control gaps that internal teams were unaware of.** Organizations that believe they have full visibility into their security posture are often demonstrating the confidence gap the assessment is designed to surface.
"A Third Eye assessment is something we do after a security incident." Post-incident reviews are valuable. Pre-incident reviews are more valuable.	**Post-incident reviews are reactive, conducted under pressure, and focused on a specific vector.** Pre-incident **Third Eye** assessments are preventive, evidence-based, and provide the insight needed to address gaps before they are exploited. The cost difference is significant.

CREST Accredited
certin Empanelled

What Independent Assessment Data Shows

Findings from Briskinfosec's assessment history across 540+ clients in 20+ countries

Healthcare — Level 2.6

Average actual security maturity in healthcare (vs. self-assessed Level 3.5)

Financial Services — Level 3.2

Average actual maturity in financial services — detection and response most common gap

Manufacturing — Level 2.3

Average maturity in manufacturing — OT/IT segmentation the most frequent finding

Technology and SaaS — Level 3.0

Average maturity in technology and SaaS — supply chain risk management the primary gap

What a Third Eye Review Covers

The review is structured across six dimensions of security program effectiveness.
Most organizations have partial coverage in each area. The Third Eye Review maps the full picture.

DIMENSION	WHAT IS REVIEWED	WHAT INTERNAL REVIEW TYPICALLY MISSES
Security Program Effectiveness	Policy completeness, risk register quality, budget vs. risk alignment, CISO reporting structure	Strategic misalignment between security investment and actual threat profile; policy drift over time
Vendor and Tool Performance	Security tool configuration quality, redundancy mapping, coverage gaps, ROI per control layer	Misconfigured tools that appear active but provide limited protection; overlapping tools consuming budget without adding coverage
Architecture Review	Network segmentation, IAM implementation, cloud posture, endpoint configuration, SIEM detection coverage vs. MITRE ATT&CK	Detection gaps in SIEM rules; incomplete segmentation; accumulated IAM over-permissioning; cloud shared responsibility misunderstandings
Policy vs. Practice Qap	Evidence of whether documented controls are consistently applied in daily operations	Controls that exist on paper but are not enforced; accumulated accumulation; change management security steps skipped under time pressure
Board Reporting Quality	Whether security metrics presented to leadership accurately reflect real risk exposure	Reporting that shows green status while material risks remain unaddressed; lack of quantified risk in board-level summaries
Risk Prioritization Accuracy	Whether the organization is investing effort in the right risks relative to actual threat profile and business impact	Over-investment in low-impact controls; under-investment in high-probability threat vectors; threat modeling that has not been updated with current intelligence

Regulatory and Compliance Context

Independent security reviews are increasingly referenced in regulatory guidance across global frameworks

DORA
EU: ICT risk management and independent testing for financial entities (Art. 25)

NIS2
EU: Security measure effectiveness and third-party assessment (Art. 21)

SEBI
India: Independent security audit requirements for market infrastructure (CSCRF)

RBI
India: Cyber risk governance and independent security assessment for banks and NBFCs

CREST Accredited
certin Empanelled

The Cost of Inaction — Prevention Costs Far Less

Typical Third Eye Assessment engagement cost: one-time investment. Average breach cost for organizations without independent validation: $4.88M per incident (IBM). The business case is straightforward.

$4.88M
Average Breach Cost (IBM)
One avoided breach at this level delivers a return on assessment investment that exceeds engagement cost by an order of magnitude.

258 Days
Average Breach Lifecycle (IBM)
Independent review identifies detection gaps that allow attackers to operate undetected. Closing these gaps reduces dwell time significantly.

30–40%
Cyber Insuranch Premium Reduction
For organizations that can demonstrate documented and independently verified security maturity to underwriters.

2–3x
Higher Compliance Remediation Cost
When gaps are found at audit time versus identified and addressed through pro-audit independent review.

CURRENT STATE (WITHOUT INDEPENDENT VALIDATION)	FUTURE STATE (AFTER THIRD EYE REVIEW)
Security maturity assessed by the same team that built the controls	bSAFE maturity score: independent, benchmarked, evidence-based
Board reports reflect internal consensus, not independent evidence	Board receives a third-party validated view of real security posture
Compliance certifications treated as proxy for security effectiveness	Compliance gaps identified before auditors identify them
Tool sprawl without independent validation of actual coverage	Tool redundancy and misconfiguration mapped with remediation priorities
Policy vs. practice gaps visible only when exploited under incident conditions	Policy vs. practice gaps surfaced and documented for controlled remediation
Cyber insurance underwriters unable to verify maturity claims independently	Insurance underwriters provided structured bSAFE score documentation
Risk prioritization based on internal judgment without external benchmark	Prioritized remediation roadmap aligned to actual threat profile and business impact

Why Briskinfosec Third Eye Review?

INDEPENDENT	DATA-DRIVEN	COMPREHENSIVE	OBJECTIVE	ACTIONABLE	FUTURE-READY
Pure assessment model — vendor agnostic and unbiased	4,800+ assessments power real-world benchmarks	7 layers, 73 controls, 6 dimensions of security effectiveness	Identifies blind spots internal teams cannot see	Prioritized roadmap with business impact and effort estimates	Aligned to evolving threats and regulatory landscape

Our Track Record. Your Due Diligence.

Figures from Briskinfosec's engagement history across clients in 20+ countries

540+
Clients Across 20+ Countries

4,800+
Security Assessments Delivered

0%
Client Breach Rate Post-Engagement

99.8%
Compliance Achievement Rate

CREST Accredited
certin Empanelled

Three Assessment Tiers.
Choose Based on Where You Are Today.

Each tier produces a bSAFE maturity score, a gap analysis, and a prioritized remediation roadmap. Scope and depth vary by tier.

1	**Rapid Assessment (5–7 Days)**	• Focused review of highest-risk control layers. • Executive summary with critical findings and quick-win remediation items. • Ideal starting point for leadership teams new to independent assessment.
2	**Standard Assessment (15–20 Days)**	• Full five-layer review across all six Third Eye dimensions. • bSAFE maturity score with industry benchmark comparison. • Prioritized remediation roadmap with 6-month implementation plan.
3	**Enterprise Assessment (20–30 Days)**	• Full scope including third-party risk, multiple business units, and regulatory compliance mapping across all applicable jurisdictions. • Board-ready executive dashboard.
4	**Ongoing Partnership**	• Annual reassessment, continuous compliance tracking, LURA portal for remediation progress visibility. • Integration with Briskinfosec security services as needed.

Share These 8 Details.
Receive a Tailored Assessment Scope Within 48 Hours.

1	Organization Name	:
2	Industry Vertical	:
3	Approximate Employee Count	:
4	Last Independent Security Assessment (Date and Scope)	:
5	Current Compliance Certifications (ISO 27001, SOC 2, PCI DSS, Other)	:
6	Key Regulatory Requirements (DORA, NIS2, RBI, SEBI, APRA, FCA, MAS)	:
7	Primary Concern or Trigger for This Conversation	:
8	Preferred Assessment Timeline	:

CREST Accredited
certin Empanelled

The Strongest Security Programs Are the Ones That Welcome a Second Opinion.

The Third Eye Review is not a test of your team. It is a tool for your team — a way to see what internal review cannot see, benchmark where you stand, and build a roadmap grounded in evidence.

Independence. Evidence. Confidence.
That's the Briskinfosec difference.

Independent Perspective
Unblased assessment that sees beyond internal assumptions.

Evidence-Based Findings
Clear, validated insights backed by real-world assessment data.

Benchmark Your Maturity
Understand where you stand against industry peers and frameworks.

Prioritized Roadmap
Actionable remediation plan aligned to risk and business impact.

Stronger Board Confidence
Independent validation that strengthens governance and trust.

Why the Strongest Organizations Choose a Third Eye Review

DIMENSION	WITHOUT THIRD EYE REVIEW	WITH THIRD EYE REVIEW
Risk Visibility	Blind spots remain hidden until exploited.	Blind spots are uncovered and addressed proactively.
Board Assurance	Board relies on internal reports and assumptions.	Board receives independent, third-party validated assurance.
Operational Efficiency	Tool sprawl, misconfigurations, and control gaps increase complexity.	Optimized controls and tools, improved efficiency and ROI.
Compliance Readiness	Gaps discovered during audits lead to stress and penalties.	Gaps identified early, audit-ready with confidence.
Cyber Insurance	Limited insurability and higher premiums.	Demonstrable maturity drives better insurability and lower premiums.
Business Resilience	Higher probability of breach, downtime, and financial impact.	Stronger resilience, reduced risk, and business continuity.

The Real Value: Peace of Mind That's Measurable.

Reduce Risk Exposure
Identify and close critical gaps before attackers exploit them.

Save Costs
Prevent breaches, reduce remediation costs, and lower insurance premiums.

Strengthen Governance
Independent assurance that elevates board confidence.

Build Long-Term Resilience
Future-ready your security program against evolving threats and regulations.

Earn Stakeholder Trust
Clients, partners, and regulators trust verified maturity.

CREST Accredited certin Empanelled

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