CERT-In's Audit Framework 2025

10 Updates Every Leader Needs to Know

Swipe to Know

sales@briskinfosec.com

CREST. Accredited

certin Empanelled

Mandatory Annual Audits

Before :

- Only critical sectors (like BFSI, telecom, select gov entities) had mandatory annual audits.

Now :

- All public & private businesses need a yearly cybersecurity audit by CERT-In empanelled pros.

This isn't just compliance. It's safeguarding your enterprise. Stay smart.

Jaya Ram Kumar Pothi
Chief Executive Consultant

sales@briskinfosec.com

CREST. Accredited

certin Empanelled

Wider Audit Coverage

Before :

- Audits mostly just checked VAPT & basic IT infrastructure.

Know your true cyber posture. Don't get caught blindsided.

Now :

- Scope's MASSIVE: 25+ areas including Cloud, AI/ML, DevSecOps, Red Teaming, IAM, SBOM, & vendor risks.

This isn't just ticking boxes; it's a 360° deep dive into your digital fortress.

sales@briskinfosec.com

CREST. Accredited

certin Empanelled

Risk-Focused Auditing

Before :

- Audits were mostly checklist -based, verifying documents, not actual security.

Now :

- It's risk-based, lifecycle-driven: plan, test, fix, retest, validate. Focus on real threats, not just policy checks.

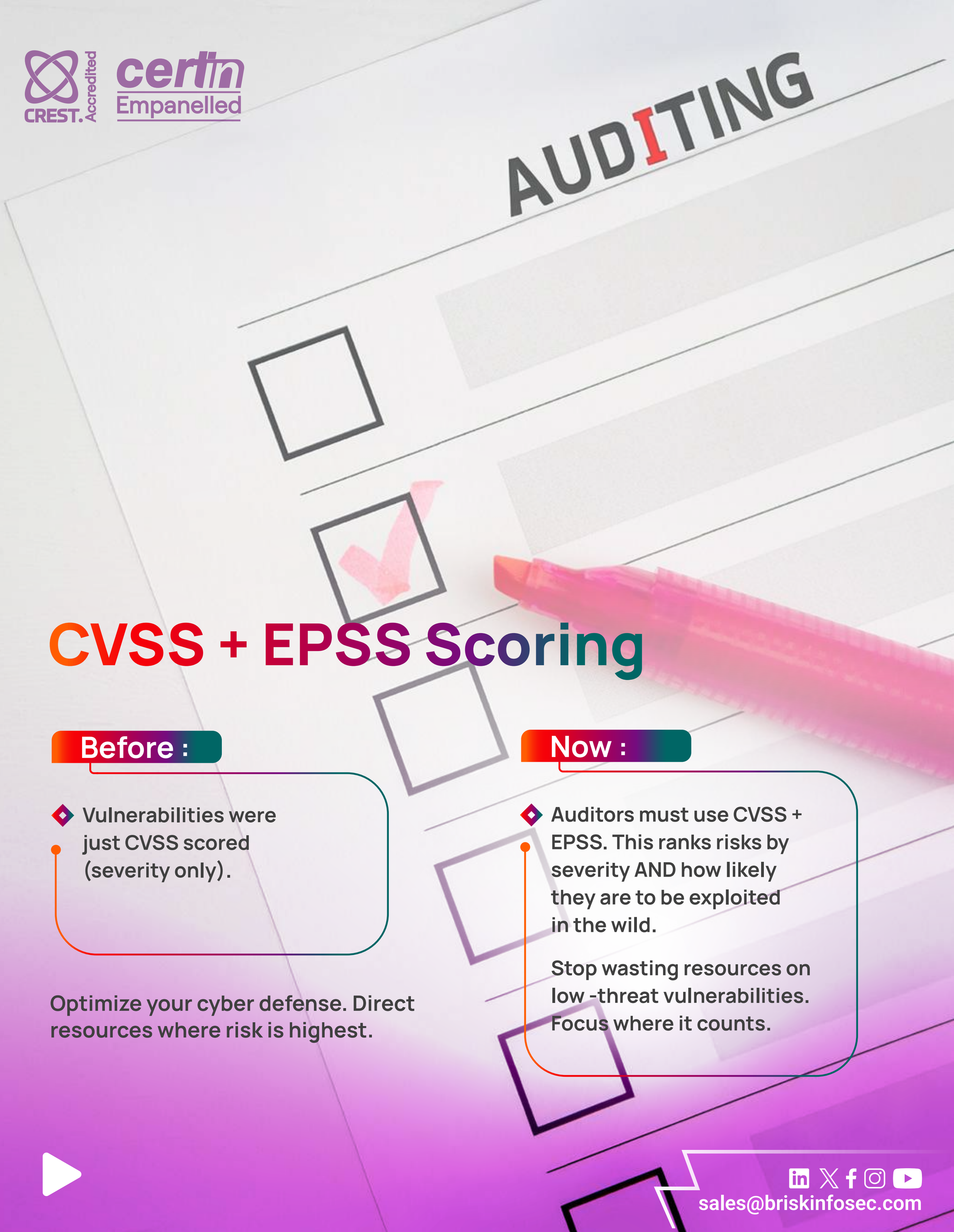
  This means proactive defense, not just reactive paperwork.

Transform compliance into a core strength. Secure your future.

sales@briskinfosec.com

CREST. Accredited

certin Empanelled



CVSS + EPSS Scoring

Before :

- Vulnerabilities were just CVSS scored (severity only).

Now :

- Auditors must use CVSS + EPSS. This ranks risks by severity AND how likely they are to be exploited in the wild.

  Stop wasting resources on low -threat vulnerabilities. Focus where it counts.

Optimize your cyber defense. Direct resources where risk is highest.

sales@briskinfosec.com

CREST. Accredited

certin Empanelled

Secure Data Handling

Before :

- No clear rules. Sensitive audit data was scattered globally, often unencrypted.

Now :

- All audit data must be stored in INDIA, encrypted, kept for 1+ year, & securely deleted post-audit.

This mandate isn't just about privacy it's about accountability & national security.

Your data integrity just got a major upgrade. Ensure compliance from day one.

sales@briskinfosec.com

CREST. Accredited

certin Empanelled

Strict Reporting Standards

Before :

- Reports were generic, lacked evidence, and had vague suggestions. No certified sign-off.

Demand clear, actionable insights.
No more guesswork.

Now :

- Reports must be detailed, evidence-based (screenshots, logs!), with clear recommendations. Certified personnel must sign off.

Transparency +Accountability
= Real cyber assurance.

sales@briskinfosec.com

CREST. Accredited

certin Empanelled

CERT-In Oversight & Submission Requirement

Before :

- CERT-In was mostly passive, getting reports late or on request.

Now :

- CERT-In can join audits! Plus, audit metadata & final reports must be submitted within 5 working days of completion.

  This means centralized monitoring & faster national risk response.

Speed is key. Align your teams for rapid, compliant submissions.

sales@briskinfosec.com

CREST. Accredited

certin Empanelled

Deter & Punish Framework

Before :

- Few penalties for poor audits or manipulation. Auditor accountability was low.

Ensure your audit partners are top-tier.
The stakes just got higher.

Now :

- CERT-In launched a penalty framework! Warnings, suspension, de-empanelment for auditors. Legal action for violators.

Integrity in audits just became non-negotiable.

sales@briskinfosec.com

CREST. Accredited

certin Empanelled

Feedback Mechanism Introduced

Before :

- No structured feedback. Concerns & improvements rarely captured.

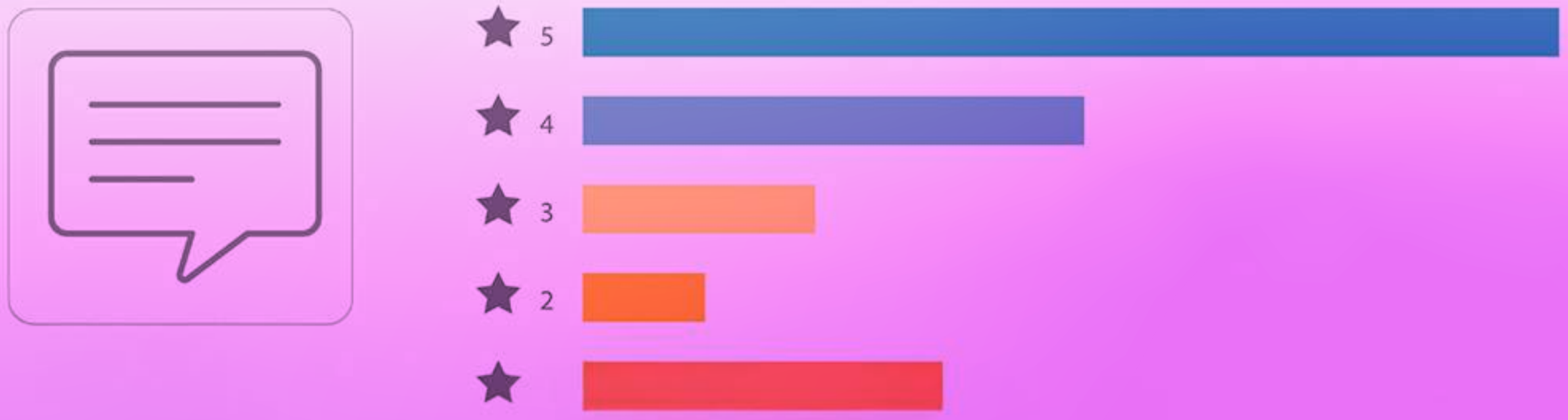
Now :

- Mandatory formal feedback loop between CERT-In, auditors, & auditees. Improves quality, transparency, & accountability.

  This means continuous improvement, not just one-off checks.

Embrace the loop. Elevate your cyber resilience through shared insights.

Feedback



sales@briskinfosec.com

CREST. Accredited

certin Empanelled

Follow-up Audits Are Mandatory

Before :

- No enforced re-audit or remediation verification. Findings often unresolved.

Ensure your remediation efforts are validated. Close the loop, close the risk.

Now :

- Follow-up audits are MANDATORY to verify fixes. An audit isn't complete until revalidation is done.

  No more "assuming" issues are fixed. It's about proven security.

sales@briskinfosec.com

CREST Accredited

certin Empanelled

BriskInfosec™

VULNERABILITY TO VICTORY

Don’t Wait. Don’t Risk It

The new audit rules aren’t just compliance checkboxes - they're your roadmap to bulletproof cybersecurity. Start today, stay ahead.

Need Expert Guidance?

Connect with Briskinfosec’s cybersecurity experts.

Arulselvar Thomas
Founder & Director

BOOK A MEETING

sales@briskinfosec.com