CREST Accredited

certin Empanelled

BriskInfosec™

Smarter Vendor Risk Management

A Step-by-Step Framework for BFSI

PHASE 1

IDENTIFY RISK

Classify vendors before access

PHASE 2

ASSESS SMART

Evaluate security before onboarding

PHASE 3

LOCK IT DOWN

Strengthen contracts & access controls

PHASE 4

CONTROL ACCESS

Enforce least privilege from day one

PHASE 5

MONITOR ALWAYS

Continuously watch, detect & respond

PHASE 6

ANNUAL REVIEW CHECKLIST

Review, reassess & strengthen continuously

sales@briskinfosec.com

CREST Accredited certin Empanelled

BriskInfosec

Phase 1

Classify Before You Assess

Not all vendors carry the same risk. Tier them first.

TIER 1 - CRITICAL

- Access to core banking, payment systems, or customer PII

Examples :
Core banking software vendors, payment gateways, cloud providers

Requires :
Full security assessment + contractual controls + continuous monitoring

TIER 2 - SIGNIFICANT

- Access to internal systems but not core infrastructure

Examples :
HR software, CRM platforms, third-party analytics

Requires :
Questionnaire-based assessment + annual review

TIER 3 - LOW RISK

- No direct system access

Examples :
Office supply vendors, facility management

Requires :
Basic due diligence only

sales@briskinfosec.com

CREST. Accredited certIn Empanelled

BriskInfosec

Phase 2

Pre-Onboarding Security Assessment

Before a Tier 1 or Tier 2 vendor gets access - run this :

- Security Questionnaire - covering data handling, access controls, incident history, certifications (ISO 27001, SOC 2)
- Document Review - request latest pen test reports, audit findings, and remediation evidence
- Compliance Verification - confirm alignment with RBI outsourcing guidelines and DORA requirements
- Reference Checks - speak to other financial sector clients if possible

sales@briskinfosec.com

CREST. Accredited certin Empanelled

BriskInfosec

Phase 3

Lock It Into the Contract

Every Tier 1 and Tier 2 vendor contract must include :

- Data Protection Clauses - how customer data is stored, processed, and deleted
- Incident Notification SLA - vendor must notify you within 24–48 hours of a breach
- Right to Audit - your team can assess vendor security posture at any time
- Sub-contractor Disclosure - vendor must declare and seek approval for any sub-processors
- Exit & Data Return Clause - clear process for data retrieval and deletion on contract end

sales@briskinfosec.com

CREST. Accredited certin Empanelled

BriskInfosec

Phase 4

Control Access From Day One

Vendor access must be strictly governed :

- Least Privilege Principle - grant only the access needed for the specific engagement
- Time-Bound Access - set expiry dates on all vendor credentials
- MFA Enforcement - mandatory for all third-party access without exception
- Dedicated Vendor Accounts - never share internal staff credentials with vendors
- Access Logging - every vendor action on your systems must be logged and reviewable

sales@briskinfosec.com

CREST Accredited certin Empanelled

BriskInfosec

Phase 5

Monitor. Don't Just Trust.

Onboarding is not the finish line. It's the starting line.

- **Real-Time Access Monitoring** – flag unusual vendor access patterns immediately
- **Threat Intelligence Feeds** – monitor if your vendors appear in breach databases or dark web listings
- **Performance & Incident Tracking** – log every security incident involving vendor systems
- **Change Notification Requirements** – vendors must inform you of significant changes to their infrastructure or personnel

sales@briskinfosec.com

CREST Accredited | certin Empanelled

BriskInfosec — Vulnerability to Victory

Phase 6

The Annual Review Checklist

- **Re-run security questionnaire** – has anything changed?
- **Review access logs** – is granted access still appropriate?
- **Request updated certifications and audit reports**
- **Reassess vendor tier** – has their risk profile changed?
- **Review contract** – do clauses still meet current RBI / DORA requirements?
- **Confirm incident history** – any breaches or near-misses in the past 12 months?

sales@briskinfosec.com

CREST. Accredited

certIn Empanelled

BriskInfosec

Don't Wait for a Vendor Breach to Test Your Framework

Third-party risk maturity is measured before an incident - not after.

BOOK A MEETING

sales@briskinfosec.com