AI-POWERED CONTINUOUS COMPLIANCE & MANAGED GRC

Threatsys GRC 360

Govern · Assess · Evidence · Certify

A multi-tenant GRC and audit-automation platform: framework scoping, control mapping, evidence collection, risk and policy workflows, collector agents and approval-gated AI compliance operations - paired with the auditors who sign off.

- **ALWAYS AUDIT-READY · PCI QSA AUTHORISED**

+91 9668200222 support@threatsys.co.in www.threatsys.co.in

THREATSYS ONE AI

Your all-in-one cybersecurity suite, extraordinarily unified

SOC, GRC, CRM, AppSec, DPDP and LMS - unified under a single roof. One platform, one login, one intelligence layer powering every layer of your security posture.

threatsys soc360 ai

AI-Native Security Operations Console

AI SIEM, SOAR, FIM and XDR fused into one AI-driven response system with threat hunting and an agentic SOC assistant.

threatsys grc360 ai

THIS DECK

Every risk. One record. All-in-one control.

Risk, policy and audit converged into one self-updating compliance cycle - audit automation, scoping and evidence.

threatsys DPDP360 ai

AI-Mastered DPDP Suite

Consent, rights, grievance SLAs, notices, DPIAs, vendor risk and evidence for the DPDP Act, 2023.

threatsys CRM360 ai

Effortless AI-powered delivery management

Every signal and interaction turned into one relationship - clients, engagements and delivery unified in one place.

threatsys appsec360 ai

Automated Application Security Testing

SAST, DAST, API testing and PTaaS with validated, evidence-backed findings across code and cloud.

threatsys LMS360 ai

Building a cyber-ready workforce

Role-based cybersecurity training, compliance awareness and practical skilling delivered at organisational scale.

FOCUS · 2 OF 6

One workspace for the whole compliance programme

Every organisation gets a portal and checklist derived from its own frameworks and scope - so the platform never shows a generic checklist to a specific client.

Govern
Policies always current

Policy authoring, approval and attestation with version history.

- Policy library
- Approval workflow
- Attestation records

Assess
Risk on one register

Risk identified, scored and tracked with owners and treatment plans.

- Risk register
- Scoring model
- CAPA tracking

Evidence
Collected continuously

Collectors and connectors pull evidence straight from your systems.

- Evidence vault
- Freshness tracking
- Control mapping

Certify
Audit-ready by default

Audits run on the same record, signed off by empanelled seniors.

- Audit workspace
- Gap and CAPA
- Executive reports

WHY A PURPOSE-BUILT GRC PLATFORM

Software alone does not pass audits

SOFTWARE-ONLY TOOLS

Automation, then a handoff

Evidence is automated - then you are left to find your own auditor.

- No assessor relationship
- Audit still a project

Generic control libraries

You interpret what your regulator actually expects.

- Thin on PCI DSS, RBI, SEBI
- Support is a chat widget

Shallow outside SOC 2

Framework coverage thins out the moment an Indian regulator is involved.

- No QSA or CERT-In depth
- Sector audits out of scope

Compliance stays a fire drill

WITH THREATSYS GRC 360

Platform and assessors together

The platform automates evidence and empanelled seniors run the audit.

- One accountable partner
- Named senior auditor

Controls tuned by assessors

Deep coverage of Indian and global frameworks in one place.

- PCI QSA, ISO, SOC 2, DPDP
- RBI, SEBI, CERT-In, UIDAI

One evidence set, reused

Allowed evidence is mapped across frameworks instead of re-collected.

- PCI DSS, ISO, SOC, DPDP together
- No duplicate client work

Audit-ready continuously, not annually

HOW IT WORKS

From gaps to audit-ready in four steps

A single guided path from first connection to a signed certificate.

01

Connect

Link cloud, identity, code and ticketing tools; the platform maps your environment.

- Scope defined once
- Applicable controls mapped
- Identity, cloud, code and tickets linked
- Asset inventory built automatically
- Only in-scope controls activated

Environment understood

02

Monitor

Controls are checked on a schedule, so drift surfaces the day it happens.

- Continuous control testing
- Failing checks flagged
- Evidence refreshed on every pass
- Owner alerted with the context
- Readiness score moves in real time

No audit-time surprises

03

Remediate

Prioritised fixes with owners and step-by-step guidance.

- Owner and due date
- AI gathers the evidence
- Guidance written by assessors
- Re-test confirms the fix
- CAPA closed with evidence attached

Gaps actually close

04

Certify

Walk into the audit with evidence already packaged and reviewed.

- Empanelled senior sign-off
- Trust Center outputs
- Evidence pack assembled per control
- Findings resolved before fieldwork
- Report and certificate issued

Certificate, not a scramble

threatsys | Your 360° Cyber Security Partner

CLIENT ONBOARDING

A client signs up once. The workspace builds itself.

Approval, scoping, workspace generation, evidence collection and reporting move as one continuous flow.

01 Tenant activation

Signup reviewed and an isolated tenant workspace provisioned.

- Identity verification
- RBAC from day one
- Storage and AI context separated
- Audit logging on from day one

Clean data boundary

02 Guided scoping

Business, people, process, technology and framework scope captured in an interview.

- Framework selection
- Asset and process scope
- In-scope systems and locations
- Third parties declared upfront

Scope on record

03 Workspace creation

Projects, checklists, controls, evidence requests and policy tasks generated from scope.

- No generic checklists
- AI assistants provisioned
- Tasks assigned to named owners
- Dashboards created per role

Ready to work in hours

04 Readiness tracking

Gaps, approvals, collector evidence, risks and CAPA tracked in real time.

- Live readiness score
- Remediation progress
- Blockers escalated automatically
- Weekly status without chasing

Always know where you stand

05 Audit decisions

Evidence-backed decisions with executive reports and compliance documentation.

- Executive reporting
- Trust Center outputs
- Certificate and report issued
- Programme rolls into the next cycle

Defensible outcomes

MODULE LANDSCAPE

A silo-free GRC ecosystem

Eight core modules on one data model - 20+ GRC and MSSP workflows, 12+ framework families.

01 Risk management

Identify, assess and monitor risk across the enterprise.

- Scoring and treatment
- Owners and due dates

02 Audit management

Plan, execute and report internal and external audits.

- Questionnaires and gaps
- CAPA and findings

03 Compliance

Monitor controls and track compliance against standards.

- Cross-mapped controls
- Readiness scoring

04 Vendor risk

Assess and monitor third-party vendor risk profiles.

- Assessments and scores
- Contract validity

05 Asset management

Track assets and their governance status.

- Ownership and criticality
- Scope linkage

06 IAM & access governance

Role management and periodic access certification.

- Least-privilege roles
- Certification cycles

FRAMEWORK COVERAGE

Multi-framework audits without duplicate work

One unified project or separate projects under the same login - with allowed evidence reused across mapped controls.

01	**Payments & cards**	Assessed by PCI QSA authorised consultants across CEMEA, Asia Pacific and the Americas. PCI DSS · PCI PIN · SWIFT CSP	**QSA-led assessment**
02	**Management systems**	Certification support from gap assessment through to the certification audit. ISO 27001 · ISO 9001 · ISO 22301	**Certification ready**
03	**Assurance reporting**	Service-organisation reporting for customers and prospects. SOC 1 · SOC 2 · SOC 3	**Customer assurance**
04	**Privacy**	Indian and global privacy obligations mapped to shared controls. DPDP Act 2023 · GDPR · HIPAA	**Privacy defensible**
05	**Sector regulators**	Indian regulatory audits run by empanelled senior auditors. RBI / NPCI · SEBI · IRDAI · UIDAI AUA/KUA · CERT-In	**Regulator aligned**

COLLECTORS & EVIDENCE VAULT

Evidence collected as work happens

Screenshots, configs and logs pulled straight from your systems and attached to the right control automatically.

Tenant-bound collectors

01

Agents and connectors scoped to a single tenant, with consent and allowlists.

- Scoped integrations
- Full connector audit history

Governed by design

Evidence vault

02

Normalised evidence stored against controls with freshness tracking.

- Reused across mapped controls
- Version and source retained
- Stale evidence flagged for refresh

One evidence set, many frameworks

Continuous control testing

03

Every control tested on a schedule, not once a year.

- Failing checks caught same day
- Drift alerts with context
- Results written straight to the control

Compliance reflects reality

Defensible audit trail

04

Every change captured as audit-ready evidence.

- Immutable action log
- Approval gates before writeback
- Who, what, when and why retained

Nothing unexplained

ALWAYS-ON INTELLIGENCE

AI agents that work while your team rests

Approval-gated assistants for risk, compliance, audit, vendor, access and policy - 10 AI employee roles in all.

01 Risk agent

Detects threats, risks and vulnerabilities continuously.

- Scores new risk
- Suggests treatment

02 Compliance agent

Detects control gaps and maintains framework compliance.

- Gap detection
- Readiness updates

03 Audit agent

Collects evidence and tracks findings automatically.

- Evidence requests
- Finding status

04 Vendor agent

Monitors third-party vendors, risk and contract validity.

- Reassessment triggers
- Expiry alerts

05 IAM agent

Watches access, roles and certification drift.

- Drift detection
- Review scheduling

06 Policy agent

Keeps policies authored, approved and current.

- Review cycles
- Attestation chasing

AUTOMATION

The manual grind, handled in the background

Testing controls, chasing evidence and tracking risk - run continuously instead of in the weeks before an audit.

Continuous control monitoring

Every control tested on a schedule so a failing check is caught the day it breaks.

- Scheduled testing
- Owner notified with context

No annual scramble

Automated evidence collection

Configs, logs and screenshots attached to the right control automatically.

- Pulled from your systems
- Freshness tracked

Evidence always current

Real-time alerts

Owners told the moment a control drifts, with the fix attached.

- Context and guidance
- No spreadsheet chasing

Faster remediation

Access reviews

Scheduled user-access certifications with an exportable record.

- Who approved what
- Segregation of duties

Access never drifts

Risk register

Log, score and track risks with treatment plans and due dates.

- Owners assigned
- Living register

Risk actually managed

Vendor risk

Third parties assessed and monitored on the same record.

- Breach notification duties
- Contract validity

Supply chain covered

BUILT ENTERPRISE-GRADE

Governance the platform enforces on itself

Multi-tenant isolation

01

Every organisation runs in its own isolated data boundary.

- Tenant-aware APIs
- Separate storage and AI context
- Tenant-scoped AI context

No cross-tenant exposure

Granular RBAC

02

Least-privilege roles down to the module and action level.

- Role templates
- Field-level restrictions
- Joiner-mover-leaver enforcement

Only what the role needs

Approval gates & SoD

03

Segregation of duties enforced through approval workflows.

- AI writeback reviewed
- Sensitive actions gated
- Dual approval on sensitive changes

Control over automation

DR, RPO/RTO & retention

04

Recovery targets and retention policies built into the platform.

- Defined RPO and RTO
- Retention and deletion rules
- Backup restore tested periodically

Resilience on record

DASHBOARDS & REPORTING

Visibility for every stakeholder

The same record read three ways - board risk, security posture and audit progress.

CEO dashboard

High-level risk heatmaps and organisational health metrics.

- Programme health
- Risk concentration

Board-ready in one view

CISO dashboard

Security compliance, threats and real-time agent alerts.

- Control status
- Open findings

Posture at a glance

Auditor dashboard

Evidence tracking, audit progress and remediation status.

- Evidence completeness
- CAPA burn-down

Audit on schedule

Readiness score

Live readiness per framework as controls pass or fail.

- Per-framework view
- Trend over time

Progress you can show

Executive reporting

Board-ready reporting across the whole programme.

- Scheduled exports
- Trust Center outputs

Reporting without rework

Trust Center

A public-facing posture summary for customers and prospects.

- Shareable assurance
- Fewer questionnaires

Sales cycles shortened

INTEGRATIONS

Compliance that reads from your real stack

The platform reads directly from your systems to test controls and gather evidence - so compliance reflects reality, not a stale questionnaire.

01	**Cloud & infrastructure**	Configuration and posture evidence pulled from your cloud accounts. AWS · Azure · Google Cloud	**Config evidence automated**
02	**Identity & SSO**	User, role and access data for certification and joiner-leaver control. Google Workspace · Microsoft Entra · Okta	**Reviews on real data**
03	**Code & CI/CD**	Change management and secure development evidence from your pipelines. GitHub · GitLab · Bitbucket	**SDLC controls evidenced**
04	**Tickets & DevOps**	Remediation and change tickets linked to controls and findings. Jira · ServiceNow · Slack	**Workflow where teams work**
05	**HR & endpoint**	Onboarding, training and device posture for people-related controls. HRMS · Active Directory · MDM · EDR / antivirus	**People controls covered**

INDUSTRIES SERVED

Built for high-stakes, regulated industries

Deployed with mid-market and large enterprises in sectors where the regulator, not the market, sets the deadline.

01 Banking & payments

Card, payment and core banking environments under several regulators at once.

- PCI DSS and PCI PIN
- RBI PSS and data localisation

Payment ecosystems secured

02 Fintech & NBFC

Fast-moving platforms that must prove control maturity to partners.

- Partner due diligence
- SOC 2 and ISO 27001

Enterprise deals unblocked

03 Government & PSU

Public digital services with CERT-In and UIDAI obligations.

- CERT-In audits
- UIDAI AUA/KUA

Public trust protected

04 Healthcare & insurance

Sensitive personal and health data across distributed operations.

- HIPAA and DPDP
- IRDAI and ISNP audits

Privacy obligations met

05 IT & services

Service providers carrying their clients compliance burden.

- Multi-framework programmes
- Trust Center assurance

Questionnaires answered

06 Retail & enterprise

Distributed estates where scope changes every quarter.

- Asset and scope tracking
- Continuous monitoring

Scope stays honest

TRACK RECORD

A platform with an audit practice behind it

20+

GRC and MSSP workflows

Onboarding, scoping, controls, evidence, risk, policy, audit and reporting in one product.

12+

Compliance frameworks

PCI DSS, ISO 27001, SOC 1/2, DPDP, CERT-In, RBI/NPCI, UIDAI, SWIFT CSP, HIPAA, VAPT and custom.

10

AI employee roles

Compliance, policy, evidence, risk, questionnaire, remediation and reporting assistants.

1,000+

Organisations served

From banks and fintechs to government, healthcare, media and manufacturing.

10+

Years of assessment experience

CERT-In empanelled testing and PCI QSA authorised consulting.

24/7

Readiness visibility

Continuous monitoring means the answer to "are we compliant" is always current.

RECOMMENDED DEMO FLOW

How to walk a client through GRC 360

threatsys | Your 360° Cyber Security Partner

Demo storyline

1 · Approve a signup and show the isolated tenant workspace appear.
Point out the data boundary and audit log starting from that moment.

2 · Run the guided scoping interview and pick two frameworks.
Show how the answers, not a template, decide the control set.

3 · Show the generated project: controls, tasks and evidence requests.
Every item has an owner and a due date before anyone starts work.

4 · Open a control and show automated evidence with its freshness date.
Then show the same evidence satisfying a control in another framework.

5 · Let an AI agent draft a policy or remediation, then approve it.
The approval gate is the point - nothing is written back unreviewed.

6 · Finish on the CEO dashboard and export the audit report.
Close on the readiness trend, not on a feature list.

Tip **Show the same evidence item satisfying two frameworks at once - that single moment is what separates GRC 360 from a checklist tool.**

ROLLOUT & VALUE

Rollout phases and client value

A practical path from tenant activation to continuous, evidence-backed compliance.

Phase 1 · Weeks 1-3

Establish

Tenant provisioned, scoping interview completed, frameworks selected and the control set mapped.

- Roles and RBAC configured
- Baseline gap assessment

Phase 2 · Weeks 4-10

Automate

Collectors connected, evidence flowing, risks registered and CAPA owners assigned.

- Continuous control testing
- Policy and access workflows live

Phase 3 · Quarter 2

Certify

Audit run on the platform record, reports issued and Trust Center published.

- Senior auditor sign-off
- Continuous readiness maintained

Client value

Audit-ready always
Evidence current, not reconstructed

One evidence set
Reused across every framework

Less manual effort
Agents do the chasing

One accountable partner
Platform and auditors together

threatsys Your 360° Cyber Security Partner

threatsys grc360 ai

Thank you

Let us scope your frameworks, connect your stack and show you an audit-ready workspace built from your own environment.

- ALWAYS AUDIT-READY · PCI QSA AUTHORISED

CALL
+91 9668200222

EMAIL
support@threatsys.co.in

WEB
www.threatsys.co.in