

The GRC & Trust Landscape

Different solutions. Different problems. Different forms of assurance.

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
Archer Enterprise <i>GRC · IRM · Operational Risk</i>	Enterprise risks, controls, compliance and resilience	Centralises enterprise risk, controls, compliance, third-party and resilience processes.	Common environment for complex enterprise risk management.	Risk registers; control management; assessments; compliance workflows; enterprise reporting	Universal compliance status; external cyber observation; software dependency discovery; network-wide verified status
AuditBoard Enterprise <i>GRC · Audit · Risk · Compliance</i>	Audit, risk, controls and compliance	Connects internal audit, risk, controls and compliance activities in one environment.	Consolidates assurance and risk-management activity.	Audit evidence; control testing; risk registers; compliance workflows; assurance reporting	Universal compliance status; external cyber ratings; nth-party discovery; cross-network verified status
BigID <i>Data Security · Privacy · Data Governance</i>	Sensitive and regulated data	Discovers, classifies and governs sensitive data across enterprise environments.	Shows organisations what sensitive data they hold, where it resides and how it is used.	Data discovery; classification; sensitive-data inventory; privacy intelligence; data-risk visibility	Enterprise compliance status; supplier compliance; cyber resilience; relationship assurance
Bitsight <i>Cyber Risk · Security Ratings · TPRM</i>	External cyber exposure and supplier ecosystems	Observes organisations externally and combines cyber telemetry with supplier-risk intelligence.	Scalable continuing visibility into third-party cyber exposure.	External cyber signals; security ratings; supplier monitoring; cyber-risk intelligence; fourth-party visibility	Internal control verification; regulatory compliance status; universal compliance status; full evidence provenance
Black Kite <i>Cyber Risk · Security Ratings · TPRM</i>	External third-party cyber exposure	Observes external security signals and translates technical findings into third-party/business-risk intelligence.	Identifies and prioritises supplier cyber exposure.	External cyber signals; security ratings; supplier risk indicators; continuous external monitoring	Internal control verification; regulatory compliance status; universal compliance status; comprehensive evidence provenance

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
Certa <i>TPRM · Third-Party Lifecycle</i>	Third parties and multiple risk domains	Orchestrates onboarding, due diligence, screening, monitoring, remediation and offboarding across the third-party lifecycle.	Automates complex enterprise third-party risk processes.	Third-party inventory; due diligence; assessments; lifecycle monitoring; risk workflows; remediation tracking	Universal compliance status; comprehensive nth-party compliance mapping; independently verified status across all relationships
Checkmarx <i>Application Security · Software Security</i>	Application code and software vulnerabilities	Tests software during development for security weaknesses across proprietary and open-source code.	Finds software vulnerabilities before deployment.	Code scanning; vulnerability discovery; SAST/SCA; application-risk intelligence; developer remediation workflows	Organisational compliance status; TPRM; data resilience; supplier assurance
Cohesity <i>Data Security · Cyber Resilience · Data Protection</i>	Enterprise data and recovery	Protects enterprise data and supports backup, recovery and cyber-resilience operations.	Protects critical data and improves recovery from ransomware and disruption.	Backup status; recovery capability; data protection; resilience signals; recovery workflows	Regulatory compliance status; supplier compliance; application security; relationship assurance
Commvault <i>Data Protection · Cyber Resilience</i>	Enterprise data, backups and recovery	Protects, backs up and recovers data and workloads across cloud, SaaS and on-premises environments.	Improves data recoverability and resilience against loss, failure and ransomware.	Backup state; recovery capability; data protection; recovery testing; resilience evidence	Enterprise compliance status; TPRM; software assurance; universal compliance status
Diligent <i>Governance GRC · Audit · ERM</i>	Governance, audit, risk and compliance	Connects board governance with enterprise risk, audit and compliance information.	Gives management and boards consolidated governance and risk oversight.	Governance records; audit management; risk registers; control oversight; board reporting	Universal compliance status; external cyber intelligence; nth-party discovery; portable relationship assurance
Drata <i>Compliance Automation · GRC · TPRM · Assurance</i>	Controls, evidence, risks, frameworks and third parties	Continuously monitors controls, manages evidence and compliance, supports audits and now provides standalone evidence-driven TPRM. (Drata)	Reduces compliance workload and supports defensible internal and third-party assurance.	Control status; evidence management; framework alignment; audit readiness; vendor assessments; TPRM decisions	Universal compliance status; complete nth-party dependency discovery; network-wide compliance mapping

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
Guardz <i>Cybersecurity · MSP Security</i>	SMB cyber exposure and attack surfaces	Gives MSPs integrated security capabilities across identity, email, devices and other attack surfaces.	Helps MSPs protect smaller organisations against active cyber threats.	Threat detection; security monitoring; endpoint/identity protection; cyber-risk signals	Regulatory compliance status; GRC system of record; TPRM assurance; network compliance status
Hyperproof <i>Compliance Automation · Risk - GRC</i>	Controls, risks, frameworks and evidence	Centralises controls, evidence, risk and compliance work across multiple frameworks.	Reduces duplicated compliance effort and coordinates compliance programmes.	Control management; evidence repository; framework mapping; risk tracking; audit readiness	Universal compliance status; nth-party mapping; external cyber observation; cross-network verified status
LogicGate Risk Cloud <i>GRC · IRM · TPRM</i>	Configurable risk and GRC processes	Lets enterprises configure workflows for ERM, cyber risk, compliance, audit, privacy and TPRM.	Digitises complex organisation-specific GRC processes.	Risk workflows; assessments; controls; compliance processes; configurable TPRM	Universal compliance status; independent external verification; software dependency discovery; network assurance
LogicManager <i>ERM · GRC · TPRM</i>	Enterprise risks and related controls	Identifies, assesses and monitors risks while connecting them with controls, policies and remediation.	Provides structured visibility of interconnected enterprise risk.	Risk registers; control mapping; assessments; remediation tracking; management reporting	Universal compliance status; external cyber ratings; nth-party dependency verification; portable compliance status
Manifest <i>Software Supply Chain · SBOM</i>	Software components and dependencies	Uses SBOMs and software-supply-chain intelligence to identify components, dependencies, vulnerabilities and associated risks.	Exposes otherwise hidden software dependencies and software-supply-chain risk.	SBOMs; component inventory; dependency visibility; vulnerability intelligence; software provenance	Organisational compliance status; enterprise TPRM; regulatory status across relationships; general business-risk assurance
MetricStream Enterprise <i>GRC · IRM · Cyber GRC</i>	Enterprise risk, controls, compliance and audit	Integrates risk, compliance, controls, audit and related GRC processes across complex enterprises.	Creates a common enterprise GRC operating environment.	Risk registers; control management; regulatory mapping; audit management; compliance workflows; reporting	Universal compliance status; independent cyber observation; nth-party discovery; reusable external status

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
NAVEX One <i>GRC · Compliance · Third-Party Risk</i>	Ethics, compliance, policies and enterprise risk	Connects corporate compliance, policies, incidents, third-party risk and reporting.	Centralises broad corporate compliance and risk programmes.	Policy management; compliance workflows; ethics reporting; third-party due diligence; risk records	Universal compliance status; software dependency discovery; external cyber posture; network-wide verified status
OneTrust <i>Privacy · Data Governance · TPRM · GRC · AI Governance</i>	Data, privacy obligations, AI, technology risk and third parties	Governs privacy and data use while also providing technology risk/compliance, AI governance and end-to-end third-party management. OneTrust now includes continuous third-party monitoring and a third-party risk exchange. (OneTrust)	Centralises governance of data and several adjacent regulatory/risk domains.	Data mapping; privacy workflows; consent; AI governance; compliance controls; third-party assessments; risk intelligence	Universal compliance status; comprehensive nth-party relationship status; software vulnerability remediation; universal relationship assurance
Oracle Fusion Cloud Risk Management <i>GRC · Financial Controls · Access Risk</i>	ERP access, transactions and financial controls	Monitors access, configurations and transactions in Oracle business processes for risk and control issues.	Automates control monitoring close to financial and ERP activity.	Access controls; segregation-of-duties analysis; transaction monitoring; financial-control evidence	Enterprise-wide universal compliance status; external cyber posture; nth-party discovery; supply-chain relationship assurance
Oracle Supplier Qualification Management <i>Supplier Management · Procurement Risk</i>	Supplier qualifications and procurement requirements	Collects supplier information and evaluates suppliers against qualification requirements.	Embeds supplier qualification into procurement decisions.	Supplier qualifications; questionnaires; eligibility criteria; procurement approval records	Universal supplier compliance; external cyber posture; nth-party mapping; independent cross-network verification
Panorays <i>TPRM · Cyber Risk · Supply-Chain Risk</i>	Third-, fourth- and nth-party cyber risk	Combines supplier assessments, external attack-surface intelligence and supply-chain discovery.	Gives organisations contextual continuing visibility across digital supplier ecosystems.	Supplier assessments; external cyber signals; attack-surface visibility; third-party monitoring; nth-party discovery	Universal compliance status; full regulatory assurance; comprehensive internally verified controls

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
Prevalent TPRM · Vendor Risk	Third-party lifecycle risk	Automates vendor onboarding, assessment, monitoring, remediation and reporting.	Provides repeatable oversight across large third-party populations.	Vendor inventory; risk assessments; due diligence; monitoring; remediation workflows; risk reporting	Universal compliance status; complete nth-party relationship mapping; software dependency assurance; universally reusable status
ProcessUnity TPRM · Vendor Risk · Cyber Risk	Third parties, controls, assessments and risk intelligence	Combines TPRM workflows with shared vendor profiles, control intelligence, evidence evaluation, external threat data and continuously updated risk scoring. (ProcessUnity)	Reduces repetitive assessment and increases the scale and depth of third-party risk analysis.	Vendor profiles; control intelligence; evidence evaluation; multi-domain risk scores; external signals; continuous vendor monitoring	Universal compliance status; complete nth-party relationship discovery; universally authoritative vendor status
Resolver ERM · Operational Risk · Incident Management	Risks, incidents and investigations	Links operational incidents, investigations and risk-management activity.	Improves operational-risk visibility and accountability.	Incident records; investigations; risk assessments; remediation workflows; operational-risk reporting	Universal compliance status; TPRM assurance; external cyber ratings; network relationship verification
Risk Ledger TPRM · Supply-Chain Risk · Nth-Party Risk	Connected supplier-security relationships	Has a shared network where suppliers maintain security profiles that customers connect to, reducing repeated questionnaires and mapping supplier relationships. (riskledger.com)	Reduces repetitive supplier assessments and exposes dependencies beyond direct suppliers.	Shared supplier profiles; security assessments; continuous supplier updates; supply-chain mapping; nth-party visibility	Universal compliance status; independent verification of every assertion; cross-domain regulatory status; comprehensive evidence provenance
Riskconnect ERM · GRC · Resilience	Enterprise risk, compliance and resilience	Consolidates enterprise risk, compliance, audit, resilience and related workflows.	Provides a common enterprise view of risk and resilience.	Risk registers; compliance records; audit management; resilience workflows; enterprise reporting	Universal compliance status; external cyber observation; nth-party discovery; portable verified status
RubrikData Security · Cyber Resilience · Data Protection	Enterprise data and recoverability	Protects and monitors enterprise data and supports recovery following cyber incidents.	Helps organisations identify data exposure and recover critical data after attack.	Data inventory; backup state; recovery readiness; data-risk signals; cyber-recovery capability	Regulatory compliance status; TPRM; software component assurance; network compliance status

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
SAI360 <i>GRC · IRM · TPRM</i>	Governance, enterprise risk, compliance and third parties	Manages policies, controls, risk, audit, incidents and third-party governance.	Provides a broad enterprise environment for GRC programmes.	Risk registers; controls; compliance workflows; audit records; third-party assessments; reporting	Universal compliance status; independent cyber observation; nth-party verification; portable network status
SAP Ariba Supplier Risk <i>Supplier Risk · Procurement · TPRM</i>	Suppliers and procurement-related risk	Performs supplier due diligence, control assessments and continuing monitoring across financial, operational, environmental, social, regulatory and legal risks. (SAP)	Brings supplier-risk intelligence directly into procurement and source-to-pay decisions.	Supplier assessments; risk alerts; ongoing compliance checks; supplier-risk exposure; issue/remediation workflows	Universal compliance status; complete nth-party mapping; application-security assurance; cross-network verified status
SAP GRC / Risk Management <i>Enterprise GRC · Risk · Controls</i>	Enterprise risk, controls and access governance	Integrates risk, controls and compliance processes with SAP-centric enterprise operations.	Brings governance and control monitoring close to core ERP processes.	Control monitoring; enterprise-risk records; access governance; compliance workflows; ERP-related assurance	Universal compliance status; external cyber ratings; nth-party discovery; portable relationship status
SAP Sustainability Solutions <i>ESG · Sustainability · Reporting</i>	Sustainability data and reporting obligations	Collects, governs and reports environmental and sustainability information connected to enterprise operations.	Supports sustainability measurement, governance and regulatory reporting.	ESG data; sustainability metrics; reporting workflows; environmental accounting; disclosure support	General GRC assurance; universal supplier compliance; cyber posture; complete supply-chain compliance status
Secureframe <i>Compliance Automation · GRC</i>	Controls, frameworks and audit evidence	Automates evidence collection and compliance management across security/privacy frameworks.	Reduces effort required to achieve and maintain framework compliance.	Control status; evidence collection; framework mapping; audit readiness; compliance monitoring	Universal compliance status; nth-party discovery; supply-chain relationship mapping; network-wide status
SecurityScorecard <i>Cyber Risk · Security Ratings · TPRM</i>	External cybersecurity posture	Uses externally observable signals and threat intelligence to rate and monitor organisations and suppliers.	Provides scalable comparative visibility into external cyber exposure.	Security ratings; external cyber signals; supplier monitoring; attack-surface intelligence; cyber-risk indicators	Internal control verification; regulatory compliance status; universal compliance status; comprehensive evidence provenance

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
Securiti <i>Data Privacy · Data Governance · Data Security · AI Governance</i>	Sensitive data, privacy obligations and AI/data governance	Discovers data and applies privacy, security, governance and AI controls across enterprise data estates.	Connects sensitive-data discovery with governance and regulatory workflows.	Data discovery; classification; privacy workflows; data controls; AI governance; data-risk intelligence	Enterprise universal compliance status; TPRM assurance; software-component security; nth-party compliance mapping
ServiceNow IRM <i>Enterprise GRC · IRM · Operational Risk</i>	Enterprise risk, controls, compliance and workflows	Connects risk and compliance across IT, cyber and business operations; continuously assesses controls and routes remediation through operational workflows. (ServiceNow)	Embeds risk and compliance into enterprise operations.	Risk registers; control testing; evidence management; compliance workflows; remediation; audit readiness	Universal compliance status; external cyber ratings; comprehensive nth-party discovery; portable external status
ServiceNow <i>TPRMTPRM · Vendor Risk</i>	Third parties and lifecycle risk	Centralises vendor risk, automates assessments, monitors changes and manages remediation from onboarding through retirement. (ServiceNow)	Gives large organisations consistent third-party oversight.	Vendor inventory; due diligence; risk assessments; continuous monitoring; remediation workflows; lifecycle records	Universal compliance status; complete nth-party dependency discovery; independently authoritative supplier status
Sonatype <i>Software Supply Chain · SCA · Open-Source Security</i>	Open-source components, packages and software dependencies	Controls software components entering development, detects vulnerabilities and malware, enforces policies and supports SBOM management. (Sonatype)	Prevents risky components from propagating through software development and improves supply-chain visibility.	Component intelligence; SCA; dependency risk; malware detection; policy enforcement; SBOMs	Organisational compliance status; enterprise TPRM; business relationship assurance; data resilience
Sprinto <i>Compliance Automation · GRC</i>	Controls, evidence and compliance frameworks	Maps requirements to controls, monitors those controls and automates evidence and remediation workflows.	Makes compliance continuous rather than periodic audit preparation.	Control status; framework mapping; evidence collection; continuous monitoring; audit readiness	Universal compliance status; comprehensive nth-party discovery; external cyber observation; network-wide relationship status

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
StandardFusion <i>GRC · Compliance Management · Risk</i>	Controls, risks, audits and frameworks	Centralises GRC activities and maps controls against regulatory and security requirements.	Makes compliance programmes and audits easier to manage.	Control management; risk registers; framework mapping; evidence; audit management	Universal compliance status; external cyber ratings; nth-party discovery; reusable network assurance
Snyk <i>Application Security · Software Supply Chain</i>	Application code, dependencies, containers and infrastructure-as-code	Finds and helps remediate vulnerabilities across proprietary code and direct/transitive software dependencies, with continuous monitoring and SBOM capabilities. (Snyk)	Helps developers prevent and remediate application and software-supply-chain vulnerabilities.	Code scanning; dependency visibility; vulnerability intelligence; SBOMs; reachability analysis; remediation guidance	Organisational compliance status; TPRM assurance; supplier regulatory status; business relationship verification
Thoropass <i>Compliance Automation · Audit & Assurance</i>	Controls, evidence, certifications and assessments	Combines compliance software, evidence management and audit/assessment services.	Shortens the path from compliance preparation to independent assessment.	Control evidence; compliance readiness; audit workflows; independent assessment where engaged; certification support	Universal compliance status; nth-party discovery; external cyber intelligence; network-wide relationship status
Vanta <i>Compliance Automation · GRC · TPRM</i>	Controls, evidence, frameworks and vendor risk	Connects to business systems, collects evidence and continuously monitors controls; its TPRM capability also tracks vendors, assessments and changing vendor risk.	Reduces manual compliance work and supports continuing audit and vendor-risk readiness.	Control status; evidence collection; framework alignment; audit readiness; vendor inventory; vendor assessments	Universal compliance status; comprehensive nth-party dependency discovery; network-wide compliance mapping
Veracode <i>Application Security · Software Security</i>	Application code and software vulnerabilities	Tests applications and software components for vulnerabilities throughout development.	Helps development and security teams identify and remediate software weaknesses before release.	Application vulnerabilities; code-security findings; software composition risk; remediation guidance	Organisational compliance status; TPRM; data resilience; relationship assurance
Workiva <i>GRC · Audit · ESG · Regulatory Reporting</i>	Reporting, controls, audit and regulatory/ESG information	Connects financial, regulatory, sustainability, audit and risk data into controlled reporting workflows.	Improves governance, traceability and collaboration around complex reporting and assurance.	Reporting controls; audit trails; ESG reporting; regulatory disclosures; connected reporting data	Universal compliance status; external cyber posture; nth-party discovery; supplier assurance

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
Resolut <i>Trust Infrastructure · Business Continuity Compliance Status - TPR - Audit Readiness SBOM Supply Chain Risk Identification</i>	Compliance status and connected relationships across people, organisations, software, systems and dependencies	Establishes requirements, validates supporting evidence and continuously maps compliance status across connected parties and dependencies, including the data supply chain.	Creates a reusable universal compliance status and exposes non-compliance, unknown dependencies, vulnerabilities and associated risk so that what was unknown can be acted upon.	Universal compliance status; validated evidence; evidence provenance; relationship mapping; nth-party visibility; unknown dependency discovery; non-compliance exposure; vulnerability/risk visibility; status reuse; revocation. Cyber Insurance	Threat prevention; vulnerability remediation; corrective-action execution; risk elimination; cyber recovery
AdaptiveGRC <i>GRC · Risk · Compliance · Audit · TPRM</i>	Enterprise risks, controls, compliance, audits and vendors	Provides modular GRC capabilities covering risk management, compliance, internal controls, audit, data protection and vendor management, with assessments, reporting and corrective actions.	Centralises GRC activities and exposes compliance gaps and risk requiring action.	Risk registers; compliance status; control monitoring; assessments; audit trails; vendor management; gap analysis; corrective-action tracking	Universal compliance status; external cyber observation; independent evidence verification; nth-party dependency discovery; portable cross-network status
Hyperproof <i>GRC · Compliance Automation · Risk · TPRM</i>	Controls, evidence, frameworks, enterprise risks and vendors	Creates a common system for compliance, risk and audit; maps controls across frameworks and now automates vendor assessments using documents, external monitoring, questionnaires and AI-based risk analysis.	Reuses control work across frameworks while connecting compliance, enterprise risk and vendor risk.	Control status; evidence management; framework mapping; risk registers; audit readiness; vendor assessments; external vendor monitoring; remediation tracking	Universal compliance status; comprehensive nth-party discovery; network-wide relationship mapping; portable verified status across independent parties

Solution	What it manages	What it actually does	Value delivered	Provides / Establishes	Does not provide
Onspring GRC <i>GRC · Risk · Compliance · Audit · TPRM</i>	Enterprise risk, controls, compliance, policies, audits and third parties	Provides a configurable GRC suite covering risk, compliance, policy, audit, incidents and TPRM. Its compliance product maps controls across frameworks and reuses evidence, while TPRM covers lifecycle assessment, monitoring and remediation.	Connects previously separate GRC programmes and automates assessment, evidence and risk workflows.	Risk registers; control testing; evidence reuse; compliance status; audit management; vendor assessments; TPRM monitoring; nth-party documentation; remediation tracking	Universal compliance status; independent verification of all supplied evidence; external cyber intelligence without integrations; network-wide portable compliance status
UpGuard <i>TPRM · Cyber Risk · Security Ratings · Supply-Chain Risk</i>	Vendor cyber posture, controls and third/fourth-party risk	Combines external security scanning, security ratings, vendor assessments, questionnaires, sourced evidence and continuous monitoring. It also identifies fourth-party concentration and supply-chain risk.	Gives buyers a continuously updated view of vendor cyber risk while reducing manual assessment work.	Security ratings; external cyber signals; vendor control status; sourced evidence; vendor assessments; continuous monitoring; vulnerabilities; fourth-party visibility; concentration risk	Universal compliance status; complete regulatory status; comprehensive internally verified controls; full nth-party relationship mapping; portable compliance status