RISKAVAIRE FAQs

Platform Overview and Getting Started

1. What is the RiskaVaire GRC platform?
   RiskaVaire is a comprehensive Governance, Risk & Compliance platform designed to integrate critical GRC functions seamlessly, transforming complexity into clarity for organizations.
2. Who operates the RiskaVaire GRC platform?
   The platform is operated by Vardaan Data Sciences Pvt Ltd, based in Hyderabad, India.
3. What are the core capabilities of RiskaVaire?
   The platform provides role-based dashboards, policy creation and versioning, compliance mapping, audit planning, incident management, risk assessment, and advanced analytics with real-time notifications.
4. What modules are available in RiskaVaire?
   Key modules include Policy Management, Compliance Management, Audit Management, Incident Management, and Risk Management functionalities.
5. What are the system requirements for using RiskaVaire?
   Minimum requirements include: dual-core 2.0 GHz processor, 4GB RAM (8GB recommended), 2GB free disk space, screen resolution 1366×768, and stable 5 Mbps internet connection.
6. Which operating systems are supported?
   Windows 10+, macOS Monterey+, and Linux Ubuntu 20.04 LTS+ on both x86 and ARM architectures.
7. What browsers are compatible with RiskaVaire?
   Latest two versions of Chrome, Edge, Firefox, Safari, Opera, and Brave with JavaScript and cookies enabled.
8. How do I get started as a first-time user?
   Receive credentials from your administrator, sign in, accept the EULA and Privacy Policy during first login, then access your role-based dashboard.
9. What support resources are available?
   Access to EULA, Privacy & Security Policies, feedback channels, and direct support team contact.
10. How does the platform ensure scalability?
    The platform features scalable design supporting large user bases with web-based interface accessible via modern browsers.

System Administration and Setup

1. Who provides administrator credentials?
   Administrators receive login credentials and license details directly from Vardaan Data Sciences.

2. What happens during the first admin login?
   Administrators must read and accept the EULA and Privacy & Security Policies before proceeding.
3. How should backup procedures be configured?
   Configure automated backups during off-peak hours, test restoration regularly, store backups securely off-site, and maintain audit logs.
4. What is the process for creating new users?
   After admin login, administrators can create users, assign roles, and share credentials with each new user.
5. How are licenses managed and activated?
   Licenses are activated only after full payment is received .
6. What data types does the platform support?
   Assessment data, audit data, issue data, KRIs, operational documents, policy data, and operational loss data.
7. How is data quality maintained?
   Through automatic consistency checks, approval workflows, and guided data entry ensuring valid input.
8. What security integrations are available?
   LDAP/Active Directory integration, role-based security framework, and audit-ready reports detailing user roles and activity.
9. How is help and support accessed within the platform?
   Through the Help Section providing documentation access, feedback channels, and direct support team contact.

User Authentication and Login

1. What credentials can I use to log in?
   You can use either your User ID or Username to access the platform.
2. Is Multi-Factor Authentication (MFA) supported?
   Yes, MFA is available for enhanced security and can be enabled during login or through profile settings.
3. What should I do if I forget my password?
   Use the "Forgot Password" option on the login screen or contact your administrator for password reset.
4. What happens during first-time login?
   New users must complete a consent form, reviewing and accepting Terms and Conditions, EULA, and Privacy & Security Policy.
5. How long do login sessions last?
   Sessions may timeout automatically for security; specific duration depends on organizational security policies.

6. Are login attempts monitored?
   Yes, all user activities including login attempts are logged for security auditing purposes.
7. How is my login information protected?
   All credentials are encrypted, and MFA provides additional security layers with secure authentication protocols.
8. What notifications are sent for login activities?
   Email notifications can be configured for login events and security-related activities.
9. How do I enable or configure MFA?
   MFA can be configured during login setup or managed through profile settings with administrator assistance.

Dashboard and Navigation

1. How is the dashboard organized?
   Dashboards are role-based, showing only information and actions relevant to your responsibilities (Risk Owner, Auditor, Admin, etc.).
2. What quick access options are available?
   Quick access to View Dashboard and View Policies, plus navigation to all assigned modules.
3. How do I navigate between modules?
   Select modules from the left navigation bar; each displays its respective submodules when selected.
4. Where are notifications located?
   Notifications are accessible from the bottom of the left navigation bar.
5. What information is shown on the dashboard?
   Statistics relevant to your role including total policies, regulations, uptime, response time, compliance rates, and risk scores.
6. How do I access different framework policies?
   Use the Policy module to navigate through frameworks, then drill down to specific policies and sub-policies.
7. Where is the logout option located?
   The logout option is positioned at the far right of the top bar.
8. Are dashboard statistics updated in real-time?
   Yes, dashboard elements provide real-time updates with refresh options available.

User Profile and Account Management

1. How do I access and update my profile?
   Click the Profile icon at the end of the left navigation bar to access Account, Role, Password, and Notifications tabs.

2. What personal information can I modify?
   First name, last name, email, phone number, department, business unit, entity, location, and department head.
3. How do I change my password securely?
   Navigate to Profile → Password tab, verify email ID, enter OTP, then set new password with confirmation.
4. Can I manage notification preferences?
   Yes, configure email, WhatsApp, and platform alerts through the Notifications tab in your profile.
5. How do I request a role change?
   Go to Profile → Role tab, enter username, select desired role from dropdown, then submit request for approval.
6. What business information can I update?
   Department, business unit, entity, location, and department head information.
7. How do I verify my contact information changes?
   Email verification is typically required for contact information updates.
8. Can I view my activity history?
   Yes, audit trails of your personal data processing activities are available in your profile.
9. Who can see my profile information?
   Only authorized personnel based on your organization's privacy policy and role-based access controls.
10. How do I save changes to my profile?
   Use the "Save Personal Info" or respective save buttons after making changes in each profile section.

Role-Based Access Control (RBAC)

1. What are some examples of predefined roles?
   System Administrator, GRC Manager, Risk Owner, Risk Contributor, Compliance Officer, Policy Owner, Auditor/Audit Team, Business User, and Third-Party User.
2. How does least-privilege access work?
   Each user receives only the minimum permissions required for their job responsibilities across all modules.
3. Can roles and permissions be customized?
   Yes, administrators can create additional roles and assign different modules and permissions based on organizational needs.
4. Who approves role change requests?
   Role changes require approval through designated workflows, typically by administrators or authorized reviewers.

5. How often are user permissions reviewed?
   Regular access reviews and privilege audits are conducted, with segregation of duties for sensitive operations.
6. What permissions do different roles have in Policy Management?
   System Admin has full access; Policy Owner can view, create, edit, and delete; Compliance Officer can view, create, and edit; Business User can only view.
7. How are permissions distributed across GRC modules?
   Each role has defined privileges across Policy, Risk, Compliance, Audit, and Incident modules with view, create, edit, approve, and delete permissions.
8. Can I see my current role and permissions?
   Yes, your current role is displayed in the Role section of your profile with associated permissions.
9. What happens if I need access to additional modules?
   Submit a role change request through your profile, which will go through the approval workflow.

Policy Management

1. What is the Policy Tree and how do I use it?
   The Policy Tree provides a visual hierarchical representation of frameworks, policies, and sub-policies relationships with expand/collapse functionality.
2. How do I create a new framework?
   Navigate to Policy Creation → Create New Framework, enter framework name, description, type (Internal/External), identifier, category, reference documents, and effective dates.
3. What is the policy approval workflow?
   After creating policies, assign a reviewer/approver who receives notifications, reviews content, and approves/rejects with feedback options.
4. Can I create sub-policies under main policies?
   Yes, add sub-policies with names, identifiers, controls (mechanisms and procedures), and detailed descriptions.
5. How does AI assist in policy management?
   AI helps with automated policy and framework content extraction from uploaded documents, parsing and mapping to compliance requirements.
6. What is policy versioning and how does it work?
   Versioning allows creating new versions of existing frameworks or policies while maintaining history; new versions require approval before becoming active.
7. How can I tailor existing policies?
   Use Tailoring & Templating to customize internal frameworks and policies, modifying details as needed before submitting for approval.

8. What happens when I modify a policy?
   Changes appear in the Policy Approval section, triggering the approval workflow and creating audit trails for tracking.
9. Can I upload existing framework documents?
   Yes, use Upload Framework feature where AI automatically extracts policies, sub-policies, and controls from uploaded PDF documents.
10. How do I track policy performance?
    Use the KPI Analysis Dashboard to monitor compliance status, acknowledgment rates, coverage rates, revision rates, and approval times.

Data Security and Privacy

1. What technical safeguards protect my data?
   Role-based access control, MFA, end-to-end encryption, secure APIs, network segmentation, firewalls, and intrusion detection systems.
2. How is data encrypted in RiskaVaire?
   Data is encrypted both at rest and in transit using industry-standard encryption methods.
3. What operational safeguards are in place?
   Regular access reviews, privilege audits, segregation of duties, audit trails, controlled data export, and secure deletion procedures.
4. How often are security assessments conducted?
   Regular vulnerability assessments, penetration testing, and security monitoring with incident response capabilities.
5. Are user activities monitored and logged?
   Yes, all user activities and data modifications are recorded in comprehensive audit trails.
6. What security standards does the platform meet?
   Role-based security framework with granular privileges, confidentiality settings, and audit-ready reports.
7. How are security patches managed?
   Regular security patches and system updates are applied to address vulnerabilities.
8. What happens during a security incident?
   Immediate containment, impact assessment, user notification within 72 hours, regulatory reporting, and forensic investigation.
9. How is data anonymization handled?
   Data anonymization and pseudonymization are applied where applicable to protect sensitive information.
10. What network security measures are implemented?
    Network segmentation, firewall protection, intrusion detection/prevention systems, and security monitoring.

Data Collection and Processing

1. What personal data does RiskaVaire collect?
   Username, email, phone number, professional information (department, business unit, role, location), MFA data, and activity logs.
2. What organizational data is processed?
   Policy documents, compliance records, audit findings, incident reports, risk assessments, business unit information, and financial impact analyses.
3. How is data collected from users?
   Through user registration, profile management, document uploads, AI-assisted content extraction, system logs, manual data entry, and external system integrations.
4. What legal basis justifies data processing?
   Contractual necessity for service provision, legitimate business interests in GRC management, regulatory compliance, and explicit user consent.
5. Does the platform support multiple data types?
   Yes, including assessment data, audit data, issue data, KRIs, operational documents, policy data, and operational loss data.
6. How does AI assist in data processing?
   AI enables automated policy extraction, risk analysis, predictive assessments, compliance gap identification, and incident impact analysis.
7. Are external system integrations supported?
   Yes, the platform can integrate with external systems and frameworks for automated data import and export.
8. How is data quality ensured during collection?
   Through automatic consistency checks, approval workflows, and guided data entry ensuring valid input.
9. What happens to manually entered data?
   Manual entries go through validation processes and are subject to the same security and audit controls as other data.
10. Is user consent always required for data processing?
    Consent is required for specific activities, while others rely on contractual necessity or legitimate business interests.

Data Retention and Disposal

1. How long is user account data retained?
   User account data is retained for the duration of active subscription plus additional years as specified in the EULA.

2. What is the retention period for audit records and logs?
   Retained per regulatory requirements and organizational policies, typically longer than user account data.
3. How can I request deletion of my data?
   Submit deletion requests through support channels, subject to regulatory and contractual constraints.
4. What happens to data when my subscription ends?
   Data follows retention policies and regulatory requirements before secure deletion.
5. How is secure data deletion performed?
   Using industry-standard secure deletion methods with verification of complete data removal.
6. Are certificates provided for data destruction?
   Yes, certificates of destruction are provided for physical media with documentation of disposal activities.
7. Who oversees data retention practices?
   Designated IT, compliance, and privacy personnel according to organizational processes.
8. How is obsolete data identified for disposal?
   Through regular review processes aligned with regulatory requirements and organizational policies.
9. What documentation is maintained for data disposal?
   All disposal activities are logged, verified, and documented with certificates where applicable.
10. Are there different retention periods for different data types?
    Yes, user account data, policy data, compliance records, system logs, and audit records may have different retention requirements.

User Rights and Controls

1. What rights do I have regarding my personal data?
   Access to your data, rectification of inaccuracies, data portability, consent withdrawal, and complaint lodging with supervisory authorities.
2. How do I access my personal data?
   Through profile sections where you can view personal information and related processing activities.
3. Can I correct inaccurate information in my profile?
   Yes, edit your profile directly or contact support for assistance with corrections.
4. What is data portability and how do I request it?
   You can request your data in standard formats for transfer to other systems; submit requests through support channels.

5. How do I withdraw consent for data processing?
   Use withdrawal options in your profile privacy controls or contact the Data Protection Officer.
6. Can I view audit trails of my data processing?
   Yes, audit trails showing your personal data processing activities are available.
7. Are there self-service privacy management tools?
   Yes, the platform provides self-service privacy management tools for user control.
8. How do I customize notification preferences?
   In your profile Notifications tab, configure email, WhatsApp, and platform alerts using toggle buttons.
9. What if my privacy request is not resolved?
   Escalate to supervisory authorities or seek legal remedies as provided by applicable law.
10. Who handles user rights requests?
    The Data Protection Officer and designated privacy contacts manage user rights requests.

Third-Party Integrations

1. Does RiskaVaire integrate with third-party services?
   Yes, it may connect with authorized third-party services for enhanced platform functionality.
2. What safeguards exist for third-party integrations?
   Third parties must maintain equivalent security standards, sign data processing agreements, and undergo regular security assessments.
3. How are third-party providers evaluated?
   They must provide transparency in data handling practices and meet the platform's security requirements.
4. What data is shared with external parties?
   Only data necessary for specific functionality, subject to user consent and contractual requirements.
5. Can I see active third-party integrations?
   Check with your administrator or organizational platform settings for integration details.
6. Is explicit consent required for third-party sharing?
   Yes, where applicable, unless sharing is contractually mandated for service provision.
7. How are users notified about new integrations?
   Via email, platform notifications, or administrative communications.
8. Can I opt out of certain third-party integrations?
   Options depend on organizational policy; consult with your administrator or support team.

9. Are subcontractors allowed for third-party services?
   Subcontracting is possible if equivalent security standards are maintained and approved by contract.
10. How often are third-party integrations reviewed?
    Regular assessments ensure ongoing compliance with security and transparency requirements.

AI and Automation

1. What AI features are available in RiskaVaire?
   AI is used for automated policy extraction, risk analysis, predictive assessments, compliance gap identification, and incident impact analysis.
2. How does AI assist with document processing?
   AI automatically extracts policies, sub-policies, controls, and compliance requirements from uploaded PDF documents.
3. Are users notified when AI processes their data?
   Yes, users are informed about automated processing activities affecting their data.
4. What AI governance measures are in place?
   Transparency in decision-making, human oversight for critical determinations, regular algorithm auditing, and bias testing.
5. Can I opt out of automated processing?
   Yes, opt-out options are provided for certain automated processing activities.
6. How often are AI algorithms reviewed?
   AI algorithms undergo regular auditing and bias testing to ensure fairness and accuracy.
7. Is human oversight available for AI decisions?
   Yes, human oversight is required for all critical determinations made by AI systems.
8. How are AI feature updates communicated?
   Significant AI updates are communicated via platform notifications or direct messages to users.
9. What transparency exists in AI decision-making?
   The platform maintains transparency as a central principle of AI governance policy.
10. Can AI help with risk assessment and compliance?
    Yes, AI assists with risk analysis, predictive assessments, and compliance gap identification.

Incident Management and Security

1. How are security incidents detected and managed?
   Through automated monitoring and manual reporting mechanisms, followed by immediate containment and impact assessment.

2. What is the timeline for security breach notifications?
   Users are notified within 72 hours of detection for significant incidents.
3. What steps are taken during incident response?
   Immediate containment, impact assessment, user/regulatory notification, forensic investigation, and system remediation.
4. How do I create and track incidents?
   Use the Incident Management module to log incidents with category, severity, impact, evidence, and link to policies or risks.
5. What incident status categories are available?
   Incidents can be Open, Assigned, Closed, Rejected, Mitigated to Risk, Approved, or In Progress.
6. Can incidents be escalated to risks?
   Yes, incidents can be escalated to the risk module for comprehensive risk management.
7. Are forensic investigations conducted after incidents?
   Yes, forensic investigation and remediation measures are standard parts of incident response.
8. How are lessons learned from incidents shared?
   Post-incident reviews lead to system improvements and may be communicated to users.
9. What training is provided for incident response?
   Staff receive regular incident response training and participate in exercises.
10. How do I access incident performance metrics?
    Use the Performance Analysis dashboard to view metrics like mean time to detect, respond, contain, and resolve.

Licensing and Legal Terms

1. What is the End User License Agreement (EULA)?
   A legally binding contract between the user and Vardaan Data Sciences outlining platform usage terms.
2. When does my license become active?
   Licenses are activated only after full payment is received by Vardaan Data Sciences.
3. What does per-user subscription licensing mean?
   Each license grants access to a single user under assigned roles and access levels.
4. Can I share my license with others?
   No, licenses are per-user and non-transferable unless otherwise approved.
5. Is reverse engineering permitted?
   No, reverse engineering, decompiling, or attempting to derive source code is strictly prohibited.

6. How do license renewals work?
   Renewal occurs upon mutual confirmation and payment of applicable fees as per agreement terms.
7. What confidentiality requirements apply?
   Software usage and related information must be treated as confidential under the agreement.
8. Who is the Licensor and Licensee?
   Vardaan Data Sciences Pvt Ltd is the Licensor; the subscribing person or entity is the Licensee.
9. What happens if license payment is delayed?
   License activation and platform access will not proceed until payment is confirmed.
10. Are there different access levels based on roles?
    Yes, role-based access control differentiates access levels (Administrator, Auditor, Compliance Officer, etc.).

International Data Transfers

1. Can my data be transferred internationally?
   Yes, with adequate protection measures, Standard Contractual Clauses (SCCs), and user notification.
2. What safeguards protect international data transfers?
   Standard Contractual Clauses, adequate protection measures, and compliance with local data localization requirements.
3. Will I be informed about cross-border data transfers?
   Yes, users are informed about transfer destinations and implemented safeguards.
4. Are local legal requirements respected?
   Yes, compliance with local data protection laws and data residency requirements are maintained.
5. Can I request specific data residency options?
   Data residency options may be available based on customer requirements for enterprise customers.
6. Who decides on international transfer destinations?
   Platform management in consultation with legal and compliance teams make transfer decisions.
7. How often are transfer mechanisms reviewed?
   Regular assessments ensure ongoing compliance with international transfer standards.
8. Can I opt out of certain international transfers?
   Options depend on organizational policy; contact your administrator or Data Protection Officer.
9. What compliance standards govern international transfers?
   GDPR for EU users, local data protection laws, and international privacy law requirements.

10. How are transfer compliance requirements monitored?
    Through regular assessment of international transfer mechanisms and legal compliance reviews.

Training and Compliance

1. What training is provided for privacy and security?
   All personnel receive initial privacy/security training, regular updates, role-specific sessions, and incident response training.
2. How often is compliance training updated?
   Training occurs at hire and is regularly updated, especially upon major policy changes.
3. What regulations does RiskaVaire comply with?
   IT Rules 2011, Personal Data Protection Bill (when enacted), GDPR for EU users, and other applicable international laws.
4. Are user guides and educational materials provided?
   Yes, users receive privacy policy guides, security communications, and self-service privacy tools.
5. How is regulatory compliance ensured?
   Through regular audits, policy reviews, compliance monitoring, and adherence to applicable legal frameworks.
6. Are incident response simulations conducted?
   Yes, incident response training includes tabletop exercises and live training simulations.
7. Is user feedback considered for compliance improvements?
   Yes, policies are updated based on user feedback and regulatory requirements.
8. Who oversees compliance within the organization?
   The Data Protection Officer, Chief Privacy Officer, and designated compliance contact persons.
9. How are staff informed about policy changes?
   Via internal communications, formal training refreshers, and system notifications.
10. What role-specific training is available?
    Security awareness and duties are matched to each user's role and responsibilities.

Support and Contact Information

1. Who is the Data Protection Officer and how do I contact them?
   Contact the DPO at info@vardaanglobal.com, +91 40-35171118, or at the Hyderabad office address.

2. How do I contact customer support?
   Use platform support features, email info@vardaanglobal.com, or call +91 40-35171118/35171119.
3. Where is Vardaan Data Sciences located?
   Aurum, 1st Floor, Plot No 57, Jayabheri Enclave, Gachibowli Hyderabad-500032, INDIA.
4. How quickly are support requests responded to?
   Response times depend on internal SLAs, with urgent queries receiving priority handling.
5. Can I escalate unresolved issues?
   Yes, escalate to supervisory authorities or seek legal remedies if necessary.
6. What information should I provide for support requests?
   Include your user ID, detailed issue description, and any relevant error messages.
7. Is there an online help section within the platform?
   Yes, the platform provides built-in FAQs, documentation, and help guidance.
8. How do I submit feedback about the platform?
   Use feedback channels provided in the Help Section or contact support directly.
9. Can I request legal remedies through the platform?
   Legal requests should be directed through official channels as instructed by the platform or DPO.
10. How are contact information updates communicated?
    Changes are announced via platform notifications, email, or direct communication.