

Operational Security & Confidence

Systems | AI | Autonomy



Achieving Security & Trust for Autonomy

The age of autonomy is here and promises to change every facet of life. Organizations seeking scale in robotics and autonomous systems must achieve and demonstrate trust in their autonomy. Rizkly is a software platform that operationalizes governance and security policies for autonomous platforms. We are a system of record and foundation for demonstrating autonomy safety and security. Without it, organizations risk erasing all of their innovation gains overnight. Rizkly enables confident adoption, protects intellectual property, ensures ethical use, and safeguards customers, turning autonomous systems from an experiment into a durable competitive advantage.

Control	IS	PP	E	G	W
VFS.01.01	●	●	●	●	●
VFS.01.02	●	●	●	●	●
VFS.01.03	●	●	●	●	●
VFS.01.04	●	●	●	●	●
VFS.01.05	●	●	●	●	●
VFS.01.06	●	●	●	●	●
VN.02.01	●	●	●	●	●

Category T1	ID T1	Name T1	Status T1	Due T1	Freq T1
Autonomous Transit Trust - Vehicle & Functional Safety					
Autonomous Transit Trust - Vehicle & Network Cybersecurity					
Autonomous Transit Trust - Cybersecurity					
Autonomous Transit Trust - AI & Autonomy Controls					
Autonomous Transit Trust - Operations & Fleet Management					
Autonomous Transit Trust - Physical Security					
Autonomous Transit Trust - Communications & Infrastructure					
Autonomous Transit Trust - Regulatory, Legal & Public Trust					
Regulatory, Legal & Public Trust	RLT.07.01	Safety case documentation	Partially Implemented	3/31/26	Weekly
Regulatory, Legal & Public Trust	RLT.07.02	Privacy controls	Implemented	6/10/26	Monthly
Regulatory, Legal & Public Trust	RLT.07.03	Transparent Incident Reporting	Planned	3/14/26	Daily

From Principles to Real-Time Response

Starting with a comprehensive and constantly updated library of AI security, risk and compliance policies and standards, Rizkly enables you to deploy tailored Autonomy Directives that instill and support your autonomy goals.

Rizkly lets you codify these policies and controls as continuous monitors that scan operational systems in real time to ensure that they are performing as defined. As potential issues are detected, Rizkly notifies and helps organizations take prompt action to mitigate risks. All monitoring statistics are visible to authorized users for streamlined governance and trust reporting.

Rizkly Spans Governance, Security Engineering & Operations for Trusted Autonomy

Rizkly's advanced Directives Engine enables real-time telemetry access, policy enforcement and continuous monitoring allowing you to demonstrate adherence to internal and regulatory requirements. Role-based access enables enterprise teams to collaborate to achieve safety & resiliency for your autonomous device fleet.



- Secure AI & Autonomy Engineering
- Autonomy Safety Testing & Fleet Maintenance
- NIST, EU, MIT, MITRE, OWASP, IEEE
- FDA Autonomous Medical Device Safety
- MAESTRO AGENTIC AI
- IEC 62304 – Medical Device Software Lifecycle
- NIST Cybersecurity
- EU Cybersecurity & Digital Sovereignty
- ISO 42001AI, 9001:2026



Policy & Governance for AI Programs, Devices and Fleets of Autonomous Machines

- Collaborative development and approval of AI/Autonomy policy and risk management
- Start from a library of AI risk, safety, ethics & security best practices from MIT, NIST, MITRE, ISO & more



Secure Robotics & AI Engineering & Testing

- Implement controls into software & engineering development lifecycle to ensure secure products
- Mitigate risks such as adversarial inputs, data poisoning, RCE, prompt injection & model inversion



Fleet Wide Monitoring & Visibility

- Automate continuous monitoring to ensure AI and autonomy policies are enforced in real-time
- Receive real-time alerts and trigger responsive action steps to mitigate risks and incidents



Machine Maintenance Management

- Implement strict maintenance training and routines to ensure safety of your autonomous fleets
- Establish autonomy maintenance programs with assigned owners, alerts and reporting



Stakeholder Confidence & Trust

- Dashboards and reports for AI and autonomy security, governance and operational performance
- Build confidence with customers, partners and regulators through our autonomy trust builder



Proven, Trusted Partner

- Rizkly is proven for enterprise, industrial & municipal use cases offering tailored support options
- FedRAMP High & DoD IL-5 Ready for local, state & sensitive federal agency/DoW workloads



About Us

Rizkly is an autonomy governance platform. We offer an enterprise software platform that lets organizations build, deploy and maintain autonomous devices and machines with the trust required to excel in the age of autonomy.

1201 Seven Locks Road, Suite 360
Rockville, MD 20854 USA
www.rizkly.com