

Clarity and Control in the Cloud

Cloud Security Assessments

Cloud environments offer tremendous agility, but without strong visibility and governance, they can quickly become high-risk. RKON's Cloud Security Assessments help you secure your cloud infrastructure by identifying misconfigurations, policy gaps, and excessive privileges, then providing prioritized recommendations aligned with your business objectives.

Our Approach

- Read-only access is provisioned for scanning and analysis, with close coordination from your cloud and IT teams
- We pair platform-native tools with manual investigation to detect misconfigurations, exposed services, and excessive privileges
- We speak with DevOps and Security stakeholders to validate findings and clarify business context
- You receive a prioritized action plan that includes remediation steps, architectural guidance, and policy recommendations

Benefits

- ✓ Spot critical gaps early
- ✓ Gain full visibility across clouds
- ✓ Prioritize risk that matters
- ✓ Strengthen posture and compliance
- ✓ Business-first risk framing tailored to your environment

Why RKON

Our engagements routinely deliver:

- Cloud-native expertise across AWS, Azure, and GCP
- Support for hybrid and multi-cloud deployments
- Fast time-to-value using proven tools and proprietary rule sets
- Executive-ready, prioritized findings every time

What We Deliver

Visibility Across Your Cloud Footprint

- Review of IaaS, PaaS, and SaaS environments
- Mapping of cloud-native controls

Misconfiguration & Policy Reviews

- Analyze security group rules, IAM roles, and storage configurations
- Validate adherence to frameworks like CIS Benchmarks, NIST, and vendor best practices
- Evaluate network segmentation and firewall controls

Identity & Access Governance

- Assess least-privilege enforcement
- Examine key rotation, MFA, and privileged account hygiene
- Validate role-based access and policy assignments

Business-Aligned Risk Prioritization

- Rank risks based on business impact
- Provide clear, actionable remediation steps
- Align recommendations with your security and compliance requirements

Strategic Recommendations

- Tailored plan for your technology stack