Dashboard Categories Overview

AiVRIC analytics are organized into the following major categories:

1. **Overview Dashboard**
2. **Findings & Risk Analytics**
3. **Compliance Dashboards**
4. **Resource & Provider Analytics**
5. **AiVRIC Vision (AI-Driven Insights & Q&A)**

Each category serves a distinct purpose and audience while integrating into a unified risk and compliance narrative.

---

1. Overview Dashboard

Purpose

The Overview dashboard provides a **high-level snapshot of security posture** across all connected providers and environments.

Key Metrics Displayed

- Percent Passing by Provider
- Total Failing Checks
- Total Resources Monitored
- Failed Findings by Severity (Critical, High, Medium, Low)
- Findings by Status (Pass, Fail, Manual)
- Daily change metrics (new vs. resolved findings)

Sample Visualizations

- Provider comparison tables
- Severity distribution bar charts
- Findings status donut charts
- Trend indicators for daily changes

Primary Use Cases

- Executive posture overview
- Rapid identification of risk concentration
- Daily or weekly security monitoring

---

2. Findings & Risk Analytics

Purpose

Findings dashboards provide **granular visibility into security issues** across providers, services, and resource types.

Core Features

- Advanced filtering by:
  - Severity
  - Status (Fail, Pass, Muted)
  - Cloud provider (AWS, Azure, GCP, Kubernetes, GitHub)
  - Region
  - Service (IAM, S3, EKS, RBAC, etc.)
  - Resource type
- Direct linkage from findings to affected resources
- Severity labeling aligned to risk impact

Key Metrics

- Open findings by severity
- High-risk and critical issues by service (e.g., IAM, S3, EKS)
- Repeated or systemic misconfigurations
- IAM-specific risk trends (privileged access, MFA gaps, root account exposure)

Sample Visualizations

- Findings tables with contextual metadata
- Severity trend charts
- Service-level risk breakdowns

Primary Use Cases

- Security team remediation workflows
- Risk review meetings
- Quarterly posture reviews

---

3. Compliance Dashboards

Purpose

Compliance dashboards translate technical findings into **framework-aligned compliance readiness scores**, enabling audit and regulatory preparation.

Supported Framework Examples

- ISO/IEC 27001:2013 & 27001:2022
- SOC 2
- PCI DSS
- CIS Benchmarks (1.x – 5.x)
- AWS Well-Architected Framework
- FedRAMP (Low / Moderate)
- HIPAA, GDPR, CISA, FFIEC, ENS, GxP

Key Metrics

- Overall compliance score per framework
- Passing vs. failing requirements
- Manual vs. automated requirements
- Top failed control families
- Section-level failure rates

Sample Visualizations

- Compliance scorecards
- Requirements status donut charts
- Top failed sections bar charts
- Failure rate heatmaps

Primary Use Cases

- Audit readiness and gap analysis
- Regulatory reporting
- Continuous compliance monitoring
- Evidence-driven risk discussions

---

4. Resource & Provider Analytics

Purpose

These dashboards provide **visibility into the underlying resources** contributing to risk and compliance results.

Key Metrics

- Total resources by provider
- Resource distribution by region
- High-risk resources by service
- Cloud-specific posture (AWS, Azure, GCP, Kubernetes)

Sample Visualizations

- Provider resource summary tables
- Region-based risk distribution
- Service-specific risk views (IAM, S3, EKS, RBAC)

Primary Use Cases

- Cloud security posture management (CSPM)
- Resource inventory and ownership alignment
- Root-cause analysis

---

5. AiVRIC Vision (AI-Driven Insights)

Purpose

AiVRIC Vision provides an **AI-powered natural language interface** that turns dashboards and findings into **executable insights**.

Capabilities

- Natural language security and compliance queries
- Contextual answers drawn from live findings and compliance data
- Executive-friendly explanations of risk and impact
- Rapid investigation without manual filtering

Example Questions

- “Are there any exposed S3 buckets in my AWS accounts?”
- “What is the risk of having unencrypted RDS databases?”
- “List my highest privileged AWS IAM users.”
- “What is my CIS 1.10 compliance status for Kubernetes?”

Primary Use Cases

- Executive Q&A
- Board reporting support
- Rapid security investigations
- Analyst productivity acceleration

Reporting & Export Capabilities

AiVRIC analytics support **exportable outputs** suitable for audits, leadership reporting, and managed services delivery.

Export Formats

- CSV
- PDF (framework-aligned reports)
- Dashboard screenshots or summaries

Typical Deliverables

- Quarterly posture review reports
- Compliance readiness snapshots
- High-risk findings summaries
- Remediation tracking reports

Summary

AiVRIC's analytics and dashboards provide **complete visibility across security, risk, and compliance**, while AiVRIC Vision transforms that visibility into **actionable intelligence**. Together, they enable organizations and managed service partners to move from reactive security monitoring to **proactive, data-driven governance**.