Quality Requirements

1. Security (Most Important)

Security is the foundation of the B.R.A.D system, given its handling of sensitive data like user-submitted URLs, forensic metadata, and potentially malicious content. Unauthorized access or breaches could lead to severe consequences such as data leaks, false reports, or misuse of the system for cyber-attacks. Therefore, security controls, encrypted storage, secure APIs, role-based access control, and container isolation must be thoroughly enforced to protect both user and system integrity.

Stimulus Source	Stimulus	Response	Response Measure	Environment	Artifact
Malicious actors/ Attackers.	Attempt to compromise data or infrastructure.	System should block unauthorized access and encrypt sensitive information.	100% of sensitive data encrypted at rest and in transit. All **RBAC (Role Based Access Control)** and **MFA (Multi-Factor Authentication)** enforced.	Production environment.	BRAD Backend/ API System

2. Compliance

Compliance ensures that the system operates within the legal and ethical boundaries defined by regulations like GDPR and POPIA. This is especially important for a tool that collects and processes potentially identifiable or legally sensitive data. Compliance includes implementing consent mechanisms, depersonalizing data when possible, logging access to personal data, and providing the right to be forgotten.

Stimulus Source	Stimulus	Response	Response Measure	Environment	Artifact
Legal/ Regulatory Bodies.	Data privacy and regulatory audits.	System should ensure legal compliance in data handling and provide user data control mechanisms.	**GDPR** and **POPIA** checklists passed; audit logs maintained; user data deletion supported.	Production environment.	Data Processing Components.

3. Reliability

The reliability of B.R.A.D ensures that forensic investigations can be conducted consistently and accurately. The system should gracefully handle failed URL submissions, avoid crashes during analysis, and recover from bot failures without corrupting data. High reliability builds trust in the system's outputs and enables analysts to depend on its results for critical decision-making.

Stimulus Source	**Stimulus**	**Response**	**Response Measure**	**Environment**	**Artifact**
System Users.	Submission of various domains, including malformed or malicious ones.	System should maintain stable operation and report errors clearly.	99.9% uptime, bot recovers from crashes within 60 seconds.	Production environment.	Bot Engine and Report System.

4. Scalability

Scalability is essential to support the analysis of many domain reports simultaneously. B.R.A.D must be able to grow with demand, especially during cyber incident spikes. It should process multiple domain submissions concurrently without bottlenecking the system or slowing down analysis pipelines. By ensuring scalability, the system can maintain optimal performance under high loads, enabling faster processing and quicker turnaround times for forensic results.

Stimulus Source	**Stimulus**	**Response**	**Response Measure**	**Environment**	**Artifact**
Multiple Users.	Submission of multiple links at the same time.	System should scale horizontally to handle multiple concurrent analyses.	Supports 500+ concurrent domain submissions with average analysis < 10s/domain.	Production environment.	Domain Analysis Pipeline.

5. Maintainability

B.R.A.D's architecture must allow for frequent updates such as patching vulnerabilities, integrating new threat intelligence feeds or adapting AI models. The system must be designed with modularity and clear interfaces between components (e.g., scrapers, AI, storage) so developers can make targeted changes without affecting the whole system.

Stimulus Source	Stimulus	Response	Response Measure	Environment	Artifact
Development Team.	Requirement to update scraping logic or AI model.	System should allow modular, low-risk updates with minimal downtime.	Docker-based components, automated deployment pipeline, <5 min rollout	Development environment.	Bot Container & AI Modules.