

Quality Engineering: Safeguarding Confidentiality, Integrity and Availability

Penetration testing and Quality Engineering (QE) reduce risks to confidentiality, integrity and availability using complementary but distinct approaches.

Penetration testing takes the attacker's viewpoint, deliberately challenging systems to expose weaknesses that could be exploited. QE testing, in contrast, is preventative and assurance-driven, checking that systems operate as designed and revealing unintended behaviours that may arise from legitimate use.

Together, these disciplines provide broader and deeper risk coverage than either approach could achieve alone.

Find out how testing can help you strengthen controls, uncover weaknesses and improve resilience, enabling your organisation to reduce information and cyber risk.



Assurance engineering

What it does

Provides independent verification that systems, controls, and processes meet defined and undefined requirements, standards, and risk controls. This ensures that the CIA of the system are being effectively upheld.

CIA impact

- **Confidentiality:** Confirms access controls, data handling rules, and segregation of duties are correctly implemented.
- **Integrity:** Verifies that data processing and change controls operate as intended.
- **Availability:** Assesses disaster recovery, resilience, and failover readiness.

Risk benefit

- Provides independent assurance that security and risk controls are effective.
- Reduces regulatory, audit, and compliance risk.
- Increases confidence in control effectiveness across the system lifecycle.

Data warehouse and big data testing

What it does

Validates large scale data pipelines, transformations, storage, and analytics outcomes.

CIA impact

- **Confidentiality:** Tests data masking, encryption, and access controls protecting sensitive data.
- **Integrity:** Ensures data accuracy, completeness, and correctness through transformations and aggregations.
- **Availability:** Confirms data platforms perform reliably under volume and peak demand.

Risk benefit

- Reduces risk of data leakage, corruption, or misreporting.
- Prevents poor data quality driving incorrect decisions.
- Supports compliance with data protection regulations (e.g., GDPR).



Device testing

What it does

Tests applications and systems across physical devices, endpoints and operating environments.

CIA impact

- **Confidentiality:** Identifies device specific vulnerabilities (e.g., cached data, insecure local storage).
- **Integrity:** Verifies data consistency across devices and platforms.
- **Availability:** Ensures services remain usable despite device, OS, or network variation.

Risk benefit

- Reduces endpoint related security weaknesses.
- Prevents data exposure caused by compromised or misconfigured devices.
- Improves system reliability for distributed and mobile users.

DevOps testing

What it does

Integrates automated testing and security controls into CI/CD pipelines.

CIA impact

- **Confidentiality:** Detects insecure configurations, secrets exposure, and access issues early.
- **Integrity:** Ensures code changes do not introduce defects, regressions, or unauthorised logic.
- **Availability:** Prevents unstable builds or faulty releases impacting live services.

Risk benefit

- Shifts risk identification left in the development lifecycle.
- Reduces likelihood of insecure or unstable changes reaching production.
- Supports secure, rapid, and controlled deployment.



Functional testing

What it does

Validates that systems work according to defined or undefined business and security requirements.

CIA impact

- **Confidentiality:** Confirms correct enforcement of roles, permissions, and data visibility.
- **Integrity:** Ensures calculations, transactions, and workflows behave correctly. Verifies system integrations to prevent data corruption.
- **Availability:** Reduces functional failures that could cause service disruption. Validates negative behaviours that ensure our system remains operational when errors occur elsewhere.

Risk benefit

- Prevents logical flaws that attackers or users could exploit.
- Reduces operational errors caused by incorrect system behaviour.
- Improves overall system trustworthiness.

Performance engineering and testing

What it does

Assesses system behaviour under load, stress, and peak usage conditions.

CIA impact

- **Confidentiality:** Prevents performance degradation that could bypass controls, expose errors or result in data leakage.
- **Integrity:** Ensures data remains accurate during high transaction volumes.
- **Availability:** Validates resilience against overload, spikes, and denial of service like conditions.

Risk benefit

- Reduces risk of outages and system failure.
- Improves resilience to high volume and malicious traffic.
- Protects business continuity and customer confidence.



Test automation

What it does

Automates repeatable tests, enabling consistent and frequent validation.

CIA impact

- **Confidentiality:** Repeatedly checks access and security controls do not drift over time.
- **Integrity:** Detects regressions or data validation issues introduced by change.
- **Availability:** Enables rapid detection of issues that could impact uptime.

Risk benefit

- Reduces human error and inconsistent testing coverage.
- Enables continuous risk monitoring in fast changing environments.
- Improves response time to emerging threats or defects.

Accessibility testing

What it does

Ensures digital products, services, and systems can be used by all individuals, including those with disabilities, by validating compliance with accessibility standards such as WCAG, ADA and Equality Act 2010.

CIA impact

- **Confidentiality:** Ensures assistive technologies do not unintentionally expose sensitive information (e.g., screen readers revealing hidden content).
- **Integrity:** Validates consistent content structure and semantic correctness to ensure information is presented accurately to all users.
- **Availability:** Ensures services remain fully usable and accessible to people with diverse abilities, improving overall system availability.

Risk benefit

- Reduces legal and compliance risk by meeting regulatory accessibility obligations.
- Prevents exclusion-related operational or reputational issues.
- Improves product usability, resilience, and user satisfaction.



Summary: Managing information and cyber risk

Across all types, Quality Engineering testing collectively:

- **Reduces likelihood** of security incidents and data breaches
- **Limits impact** of failures through early detection
- **Improves control effectiveness** across people, process, and technology
- **Supports regulatory compliance and audit readiness**
- **Strengthens organisational cyber resilience**