DXC Technology Quality Engineering - Security Quality Assurance & Testing

G-Cloud 15

Service Definition Document

Table of Contents

1 Company Overview

DXC Technology helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds.

The world's largest companies as well as mid-sized clients and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. We have a long heritage in data center services and management, operating over 320 global data centers and supporting 1,300+ customers. DXC provides innovative solutions to customers by leveraging strong domain capabilities and by applying leading technologies as represented in the DXC Technology stack below.

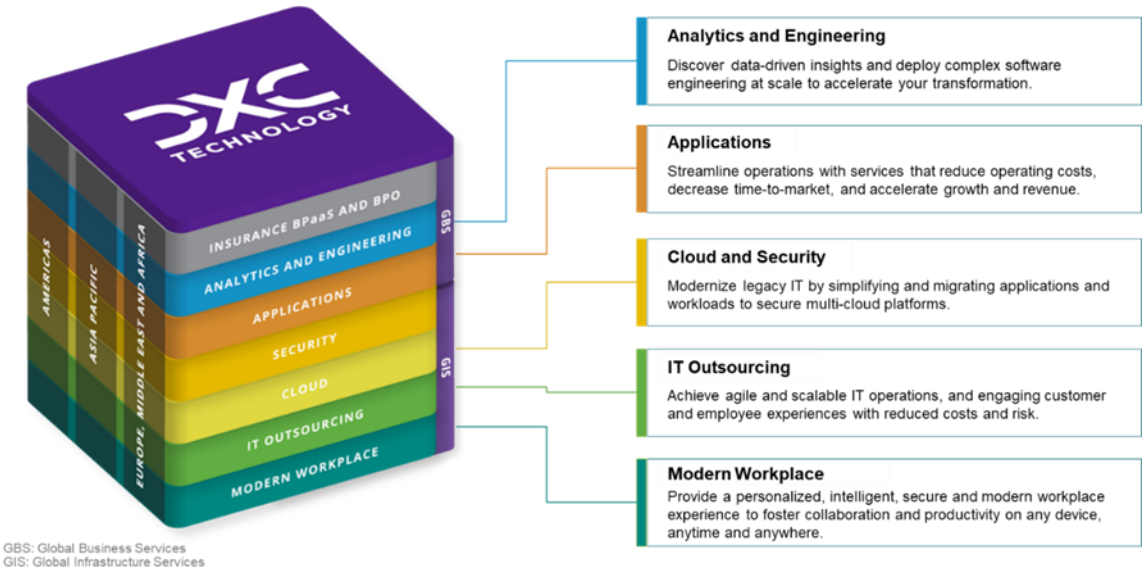

Figure 1. DXC Technology stack

DXC is one of the few IT services providers that can orchestrate mainframes, servers, private and public clouds as an effective whole. We manage the complexities of your cloud migration strategy and apply modern operating models, practices and capabilities to build and optimize cloud for the unique needs of your enterprise. We leverage deep cloud expertise and intelligent automation to run and maintain your infrastructure, and enable business agility, resilience, and continuous improvement.

1.1 Why DXC?

DXC Technology's Penetration Testing Team has UK Security Cleared consultants to a high level of vetting, the Service and Consultants are CHECK Scheme 'Green Light' and 'CREST Approved' accredited and are amongst some of the most highly qualified consultants in the industry.

2 Service Overview

DXC Quality Engineering delivers end-to-end testing services and quality management solutions that help our clients achieve seamless technology transformation from traditional to digital enterprise.

Clients improve the quality of their applications through **faster, better, continuous and more cost-effective** testing of their software.

Testing services and options to be discussed upon engagement.

DXC Quality Engineering services are tooling agnostic and are supported by Partnership with all leading providers to select and use the best tooling for the clients circumstance; we can also use the existing client tools.

Examples of partners with DXC to facilitate and expedite the services are shown below.

Figure 2. Example Service Partnerships

Each tool is designed to address different aspects of modernization, from rapid assessments and application portfolio optimization to cloud-native accelerators and mainframe transformation.

DXC is accredited to provide Penetration Testing Services on behalf of NCSC through the UK Government's NCSC CHECK Scheme, is CREST Accredited and retains a high number of experienced and accredited Penetration Testing consultants able to deliver all types of engagements including but not limited to traditional physical infrastructure, hybrid and cloud infrastructure, Web applications and remote or local on-site engagements and has a wide portfolio of services.

2.1 What the service is

DXC's Penetration testing service is the engagement of Experience and qualified, Penetration testing consultants to deliver a range of penetration testing services:

- Infrastructure Penetration Testing
- Web Application Penetration Testing
- CHECK IT Health Checks (ITHC)
- OS Build Reviews
- Firewall Config Reviews
- AWS Config Reviews
- Azure Config Reviews
- Wireless Penetration Testing
- Vulnerability Scanning
- Vulnerability Assessments
- Red Teaming
- Phishing attacks

- Cyber Attack Simulations
- CIS Benchmark assessments

Each engagement will commence with a Scoping session where we seek to understand the systems under test, the approach required, how we may connect etc and help customer stakeholders to understand how best to setup and prepare for the testing phase.

Testing Phases can include one of many of the above listed services and be approached in one of a Black, Grey, or White box method. The testing team will maintain regular contact with client teams to ensure smooth running of testing and reporting on major findings as they are discovered.

Reporting phase follows testing where the documented findings of the testing are portrayed in Exec, Technical Summary and Detailed seconds with recommendations for remediations for each finding.

2.1.1 Application Security on Demand

DXC provides consumption-based applications security testing using automated testing tools backed by DXC experts who audit the test results to remove false positives. The Applications Security on Demand services include:

- Static Security Testing: Static assessments provide security scanning, auditing, and reporting on different programming languages. Using the industry-leading tool, source code analysis of applications is completed with expert validation and reporting. Static Security Testing reviews applications in a non-runtime environment, examining the software's input and outputs that cannot be seen through dynamic web scanning. It currently supports a variety of development languages. Users can simply and securely upload source code files.
- Dynamic Security Testing: Dynamic assessments provide security scanning, auditing, and reporting for any web-based application in an active environment. Dynamic scan and analysis, or black-box testing can be performed on applications developed in all web languages. Dynamic security testing is used on active web applications during runtime to identify vulnerabilities and security issues.
- Software Composition Analysis: This service can be included as part of a static scan to identify vulnerabilities in open-source components and libraries used by the application.

2.1.2 Comprehensive Applications Threat Analysis service (CATA)

DXC's CATA service reduces the risk of introducing undiscovered (latent) vulnerabilities and security defects during the application development lifecycle. It can also be applied after development to identify future security updates that can be applied to the application or to provide an assessment of security vulnerabilities at the requirements, architecture, and design level. As more vulnerabilities and exploits of those vulnerabilities are discovered, protecting your critical data becomes a never-ending battle. CATA reviews are necessary to determine if the current application architecture and high-level design remain secure.

DXC's security consultants leverage proprietary framework and toolkits to deliver CATA services. CATA begins with a Security Requirements Gap Analysis (SRGA), which is an analysis of an application to map often-missed regulatory security requirements into technical security requirements. The output is a prioritised and vetted list of security requirements, control gaps, and an action plan to remediate.

The next CATA step is an Architectural Threat Analysis (ATA), an analysis of an application architecture and high-level design to identify changes to reduce the risk of latent security defects to a uniform acceptable level. The output of this step is a prioritised and vetted list of threats and an action plan to remediate.

2.2 Business Continuity and Disaster Recovery

A Certificate of Authorisation is required to be signed prior to any engagement which advises on Business Continuity message to take place prior to any testing commencement.

2.3 Service constraints

As standard, Denial of Service testing is not performed, and boundaries of testing are requested to be defined.

An engagement cannot legally commence without the above-mentioned Authorisation.

3 Benefits of DXC's Service

Penetration Testing is the act of ethically assuming the role of and attacker / adversary / malicious user / hacker with the aim of identifying Security Vulnerabilities and exploiting them to understand how exposed to attack a target or set of targets may be and to provide a report describing those vulnerabilities and how that were used to gain access or retrieve data, categorised in terms of risk level from Low to Critical.

3.1 Benefits

This service can form part of an Accreditation Submission, provide Audit Compliance evidence or advise on the security posture of a target environment or solution.

In understanding the security vulnerabilities and what mitigating actions can be taken to reduce the attack surface or perceived risk levels of attack, an organisation can reduce any risk of service impact, reputation impact, industry fines and loss of earnings that could be experienced as a result of a Cyber Attack.

Table 1. Benefits of DXC's service

Business Challenges and Needs	DXC Solutions and Benefits
Risk/Compliance • Skills shortages • Multiple channels, devices, and technologies niche skills need • Diversified regulatory and compliance requirements	**Solutions** • Comprehensive Applications Threat Analysis (CATA) • Static and dynamic application security testing • Application security On Demand • Mobile apps testing • Big data and analytics testing • Performance testing • Crowd testing • Usability testing **Benefits** • Multiple channels, devices, and technologies niche skills needs • Diversified regulatory and requirements compliance