ACL Digital
an ALTEN group company

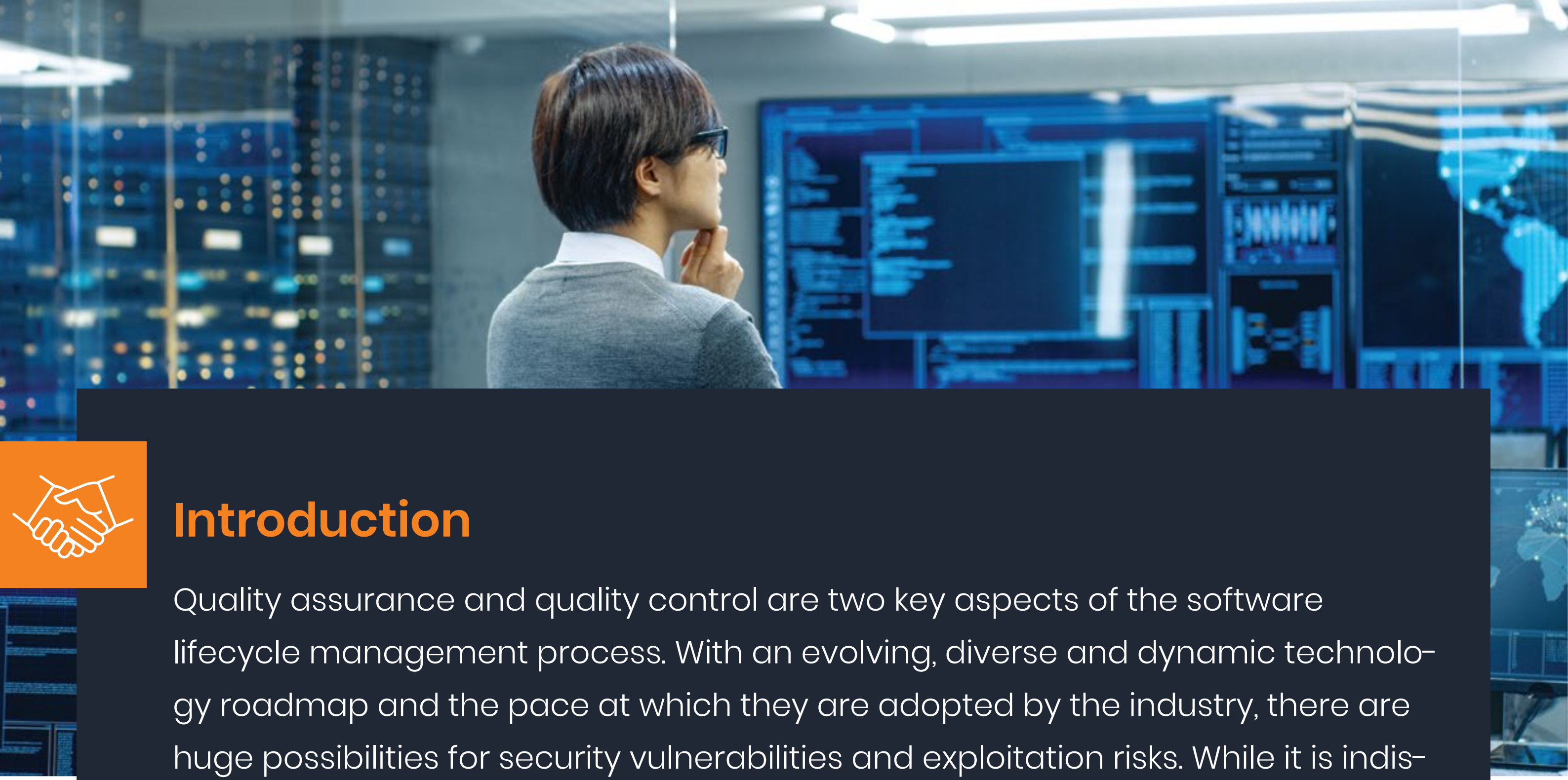
Verification and Validation

Industry leading practices for secure verification and validation of the Software Lifecycle Management process

Phase 04 of Software Lifecycle Management

Digital Product Engineering Services

Table of contents



Introduction

Quality assurance and quality control are two key aspects of the software lifecycle management process. With an evolving, diverse and dynamic technology roadmap and the pace at which they are adopted by the industry, there are huge possibilities for security vulnerabilities and exploitation risks. While it is indispensable to build enterprise applications by following the principles of secure by design, privacy by design and compliance by design, it is equally indispensable to validate and verify the outcome to ensure that the principles and best practices are adequately followed.

Security testing for the entire application portfolio needs to be automated and included as part of the organisation strategy for regulated digital transformation. This will help the enterprise in becoming more secure and establish a security maturity baseline with which the application portfolio should always comply.

There are few highly recommended use cases where security testing must be performed and for other use cases, even though optional, could also be considered keeping the risk impact in mind.

Security use cases include vulnerability and security configuration assessments (SCA) for risk identification, tracking and monitoring compliance with standards and regulations.

Key vulnerability assessments (VA) that help validate and remediate the organisation's security profile are stated as below:

1 Security configuration assessment (SCA)

This is an important feature of vulnerability assessment (VA) and provides deep insight into the configuration of systems in an environment in addition to vulnerability assessment. SCA needs to be setup as a recurring time-bound process in order to evaluate misconfigurations, exploit areas, attack surface, and unhardened systems.

2 Cloud security posture assessment (CSPA)

The gradual shift of workload from traditional computing systems to the cloud infrastructure and platform services (CIPS) has made it easier for assessing one "golden image" instead of multiple environment setups. The possibility of duplicating deployments for these CIPS container images makes it easier for performing security assessments and hardening them for repeated use.

3 Operational technology assessment (OTA)

With increased adoption of infrastructure-as-code (IaC) deployments, no-code and low-code application platform (LCAP) deployments, chatbots, 3D printers, augmented-reality (AR), virtual-reality (VR) and mixed-reality (MR) systems, and other platform solution deployments make operational technology security assessments more significant. Gartner predicts[1], by 2025, 75% of operational technology (OT) security solutions will be delivered via multifunction platforms interoperable with IT security solutions.

4 Penetration testing (Pentesting)

Pentesting is slightly different from general vulnerability assessment in the sense that it offers a validation mechanism where the application (under test) is subjected to an intense vulnerability and weakness exploitation validation in a fixed time-bound manner. Pentesting proves beneficial for providing early remediation for possible exploitation scenarios and prepares the environment for protection from exploitation attacks.

5 Citizen security testing (CST)

Sometimes it is desired to gain a neutral, outside view of the public facing enterprise applications. In such cases, internal security validation tools may not succeed in judging the impact triggered by external exploits. This is when crowdsourced validation helps with bringing in external stakeholder view and perform a more robust and intensive cross-application security testing. In some cases, business critical organizations sometimes place a bounty for such testing programs as it attracts good talented pool of security testing personnel. The competition often brings out better outcomes as opposed to more focused externally simulated security testing programs. The breach and simulation tools help add an attacker's view and validate how resilient the execution environment is, and how effectively it holds up against such simulated attacks.

Gartner proposes the following critical capabilities for application security testing[2]

1 **API testing and discovery**
All APIs are to be tested for vulnerabilities, spread of PII data, token-based access, authentication hacks, information logging, etc.

2 **Container security scanning**
Containers are to be validated for whether containers are hardened, third-party OSS libraries are scanned for vulnerabilities, container images are hardened, container workload protection platforms (CWPP) are used, etc.

3 **Dynamic application security testing (DAST)**
This helps in validating the security vulnerabilities and risks during the execution phase of the application.

4 **Fuzzing**
Inputs to an application are randomized, and uncertainties are introduced to check the integrity of execution. This includes testing application crashes, memory / storage overflows, abnormalities, to ensure that the application handles such cases gracefully without exposing sensitive information.

5 **Infrastructure as code (IaC)**
Utilizing infrastructure resources on the cloud for compute, network and storage, as source-code reduces the ingestion of vulnerabilities by external unauthorized users. Verification must be made over a course of time to check which resources can be transformed from declarative constructs to source-code based utilization.

6 **Interactive application security testing (IAST)**
This is to examine the internal working of an application during execution. An agent configured on the application server examines the code, behavior, memory/storage usage and data flow of each application run during the day.

7 **Mobile application security testing (MAST)**
This involves identifying vulnerabilities in mobile applications using static or dynamic or interactive application security testing. It also validates the interaction of the mobile frontend application with the backend services, data flow and usage of mobile device resources.

8 **Software composition analysis (SCA)**
This capability evaluates how the application security testing (AST) reports verify open-source and external dependencies are free from vulnerabilities.

9 **Static application security testing (SAST)**
Tools offering SAST capability examine critical vulnerabilities by skimming through millions of lines of application source-code. They can identify buffer overflows, SQL injection, cross-site scripting, and recommend possible mitigation techniques.

Vulnerability prioritisation technology (VPT) tools help organisations in consolidating results from multiple VA tools and present an aggregated risk score dashboard. It is highly recommended to continuously monitor this risk index to work out strategies for reducing the impact.

More targeted application security testing can be conducted during the software development lifecycle (SDLC) process:

1. **Unit testing —** The individual methods and functions of the classes, components or modules used by your product or application can be tested for PII data leakage or spread, web-service calls violating authentication and authorisation policies, inadequate documentation, etc.

2. **Functional testing —** Validate the security and data protection aspects of the business requirements and maintain end-end traceability.

3. **Integration testing —** Validate the security parameters necessary for ensuring all the modules and services work together cohesively in a secured manner.

4. **Regression testing —** This is to ensure that the application doesn't introduce newer vulnerabilities or security risks after requirement changes are applied to an existing application.

5. **Acceptance testing —** Ensure verification sign off from the security officer every time an application is released to the market.

6. **Performance testing —** Ensure that the performance of the application is not affected due to the setup of various security control measures.

Compliance testing for data protection measures

Depending upon the data protection regulation being adopted by the application, you may apply the following recommendations for validating the measures in use –

1. Validate availability of a legal basis for capturing personally identifiable information (PII). These include user consent, data processing agreement between the data controller and the data processor, user preferences, double opt-in consent, etc.

2. Validate applicability and strength of field-level and table-level encryption algorithms.

3. Validate whether minimalized PII is being captured and managed.

4. Validate the applicable retention period of PII within the application data stores as well as on the application deployment infrastructure (cloud or on-premise).

5. Validate whether end-user requests for erasure, modification and removal is actively pursued.

6. Validate whether data subjects are adequately informed about the exact business purpose for which their PII is being captured and processed.

7 Validate whether multiple copies of user PII is captured and maintained across multiple applications or internal systems. For e.g., user PII captured via applications as well as stored in the CRM are treated as multiple copies.

8 Validate whether the user PII is stored within the same geography or different geographical locations across primary storage, secondary storage, backup storage and disaster recovery sites.

9 Validate whether the application maintains an additional layer of application cache for user PII in which case it would be treated as multiple copies and for which there needs to be a legal basis.

10 Validate whether user PII is exported or imported in pure text form and later how is it stored and for how long.

11 Validate whether user PII is used for AI/ML purposes and whether such processing has been informed back to the data subject.

12 Validate how the delete user PII process is setup; whether original data are completely erased from the application infrastructure and other copies are anonymized.

13 Validate how user PII is transferred, in pure text form or in encrypted mode.

Conclusion

The IT leaders must keep their focus in ensuring a strong and secure DNA culture for the organisation, and contiguously improve the maturity index of the security baseline. Define key metrics, involve key stakeholders and combine results from multiple VA tools into a dashboard for continuous monitoring of the organisation's security risk index.

Recommended Reading

Software Lifecycle Management Infographic

Phase-01: Requirement Lifecycle Management

Phase-02: Secure Architecture and Solution Design

Phase-03: Continuous Integration, Continuous Delivery (CI/CD)

References

- [1] Gartner Market Guide for Operational Technology Security, January 2021
- [2] Gartner Critical capabilities for application security testing, April 2022
- International Institute of Business Analysis: https://www.iiba.org/knowledgehub/business-analysis-body-of-knowledge-babok-guide
- Open Web Application Security Project® (OWASP) Top 10: https://owasp.org/Top10/A00_2021_How_to_use_the_OWASP_Top_10_as_a_standard/
- General Data Protection Regulation, Europe: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- Privacy enhancing technologies: https://en.wikipedia.org/wiki/Privacy-enhancing_technologies
- NITS Cybersecurity Framework: https://www.nist.gov/cyberframework/online-learning/components-framework
- HITRUST CSF Framework: https://hitrustalliance.net/product-tool/hitrust-csf/
- https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest
- https://docs.microsoft.com/en-us/azure/architecture/patterns/sidecar
- Gartner Report: Predicts 2022: APIs Demand Improved Security and Management
- Gartner Report: Top Strategic Technology Trends for 2022
- OWASP Top 10: https://owasp.org/Top10/
- Gartner report: 2021-2023 Emerging Technology Roadmap for Large Enterprises
- OWASP Top 10 Low-code/no-code security risks

ACL Digital is a design-led Digital Experience, Product Innovation, Engineering and Enterprise IT offerings leader. From strategy, to design, implementation and management we help accelerate innovation and transform businesses. ACL Digital is a part of ALTEN group, a leader in technology consulting and engineering services.

business@acldigital.com | www.acldigital.com

USA | UK | France | India