The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 105-112
DOI 10.37547/tajet/Volume07Issue04-14

Check for updates

Fundamental Principles of Cybersecurity in The Software Testing Process

Ivanchenko Yevhenii

Caremetx, SDET Ponte Vedra, USA

OPEN ACCESS

SUBMITTED 21 February 2025
ACCEPTED 18 March 2025
PUBLISHED 21 April 2025
VOLUME Vol.07 Issue 04 2025

CITATION

Ivanchenko Yevhenii. (2025). Fundamental Principles of Cybersecurity in The Software Testing Process. The American Journal of Engineering and Technology, 7(04), 105–112. https://doi.org/10.37547/tajet/Volume07Issue04-14

Abstract: The study examines the principles of ensuring cybersecurity during software testing. The focus is placed on the fact that testing should not be limited to validation checks but must also incorporate risk assessment, compliance with standards, and early-stage vulnerability analysis throughout the software development lifecycle. The study reviews key regulatory requirements (GDPR, HIPAA, PCI DSS, ISO/IEC 27001, NIST Cybersecurity Framework) and analyzes their impact on testing strategies and quality control processes. Special attention is given to the CIA triad (confidentiality, integrity, and availability) and proactive incident planning. The necessity of integrating automated tools (SAST/DAST, SIEM, RPA, etc.) and artificial intelligence algorithms is substantiated to optimize protection procedures and enhance vulnerability detection efficiency. The conclusions emphasize that achieving a high level of product resilience is only possible through the close alignment of security requirements with test scenarios and the continuous refinement of testing methodologies. The findings presented in this study will be of interest to researchers and professionals in information security, software testing specialists, and developers seeking to integrate advanced methods into the protection of information assets.

Keywords: cybersecurity, software testing, compliance, risk management, automation, CIA triad, standards integration, artificial intelligence.

Introduction: The advancement of digitalization in everyday life has led to an increase in cyberattacks and data breaches, resulting in significant reputational and financial risks for organizations. According to a report by Gen Digital, one of the leading software developers behind antivirus programs such as Norton, Avast, and Avira, the number of cyberattacks increased by 46% in

2024 compared to 2023. Despite a decline in cybercriminal activity by approximately 7% in the second quarter, around 28.8% of active users faced cyber threats. The report states that between April and June 2024, approximately 3.05 billion cyberattacks were blocked, which is 10.6% fewer than in the first quarter. The number of blocked URLs increased by 23.6%, reaching 643 million. Analysts highlighted that approximately 95% of all cyberattacks occur through internet browsers [2].

Software testing plays a crucial role in this context, as it enables the timely identification and remediation of vulnerabilities before a product is deployed for use. Ensuring information security requires a focus not only on technical aspects but also on legal standards (GDPR, HIPAA, PCI DSS, ISO/IEC 27001, NIST, etc.).

This study provides a comprehensive review of contemporary research. Folorunso A. et al. [1] explore the relationship between security compliance and cybersecurity effectiveness, offering an empirical analysis of regulatory frameworks and statistical data to support the hypothesis that stricter compliance controls reduce vulnerabilities. Carter W. A. and Crumpler W. D. [5] analyze cybersecurity requirements in the financial sector of the Asia-Pacific region, demonstrating that adapting international standards to local conditions can enhance system resilience. Stevens R. et al. [6] examine digital standards in the United States, emphasizing the gap between regulatory requirements and real-world operational conditions, while Taherdoost H. [7] reviews existing frameworks and highlights the need for further adaptation. Huising R. and Silbey S. S. [9], along with Marotta A. and Madnick S. [10], expand on this topic by addressing contradictions between regulatory mechanisms and organizational needs. Hamdani S. W. A. et al. [11], Nazarova K. et al. [12], and Kaplan B. [14] focus on the lack of practical models for integrating security standards into testing processes. Williams B. and Adamson J. [13] conduct an in-depth examination of PCI standards, emphasizing the necessity of a systematic approach to closing gaps in existing regulatory methodologies.

The publication "Number of Cyberattacks Increases by 46% in 2024" [2], available on the Coinspaidmedia website, provides statistical data on the frequency of cyberattacks.

Machireddy J. R., Rachakatla S. K., and Ravichandran P. [3] propose a framework for integrating artificial intelligence and machine learning into analytical processes, which improves the accuracy of vulnerability detection. Mohamed S. A. et al. [4] explore robotic process automation for optimizing internal processes, supporting the hypothesis that digitalization can enhance testing efficiency. Alshaikh M. and Adamson B. [15] focus on modeling employee behavior to develop a security-conscious corporate culture, proposing a methodology that transforms security awareness into practical protective measures.

A distinct area of research focuses on cybersecurity in cyber-physical systems, as examined by Zografopoulos I. et al. [8]. This study presents a comprehensive threat assessment model for the energy sector, where scientific novelty lies in the synthesis of traditional testing methods with modern risk management approaches. The authors hypothesize that integrating case studies with comparative analysis of different methodologies significantly enhances the resilience of cyber-physical systems. Their methodology is based on empirical analysis of specific cases and the development of risk assessment metrics.

A key research gap lies in the fact that, despite the extensive number of studies discussing security, standards, and regulatory frameworks (GDPR, HIPAA, PCI DSS, ISO/IEC 27001, etc.), the integration of security requirements directly into the testing process remains underexplored. This includes the development of test scenarios, management of test data, and analysis of results.

The objective of this study is to examine existing principles of cybersecurity in the software testing process.

The scientific novelty of this research lies in the proposal of a systematic approach to software testing, in which:

- Compliance requirements are treated as an integral part of the testing methodology rather than a separate process.
- Fundamental cybersecurity principles (risk-based approach, data protection, incident response planning, continuous vulnerability assessment) are adapted to testing environments.
- Roles and responsibilities of stakeholders (testers, developers, security specialists, and project managers) are clearly defined in alignment with international standards.

The central hypothesis is that integrating cybersecurity principles into the testing process enhances overall software resilience against threats and optimizes vulnerability detection through close coordination between testing teams and information security specialists.

1. The role of cybersecurity principles in shaping

testing strategies

Modern industry standards (GDPR, HIPAA, PCI DSS, ISO/IEC 27001, NIST Cybersecurity Framework, etc.) directly influence the entire software development lifecycle, including testing. Security is often viewed as a final "quality control" measure before release; however, the most effective approach involves identifying vulnerabilities and ensuring compliance at the design and testing stages.

Without clearly defined principles and continuous oversight, testing procedures may focus solely on functional quality aspects while overlooking unauthorized data access threats. As a result, security may become selective, where certain measures, such as database encryption, are enforced, while others, such as access control and authentication, remain neglected. The key objective at this stage is to determine which specific regulations apply to the project and assess their applicability in testing scenarios. For example, the financial sector (PCI DSS) prioritizes payment data protection, while the healthcare industry (HIPAA) emphasizes the confidentiality and integrity of personal medical records [5, 14].

Developing a unified testing strategy that incorporates cybersecurity principles requires establishing internal regulations and procedures. Research by Huising R. and Silbey S. S. [9] indicates that without detailed role distribution (who configures the test environment, who controls data access, who audits test results), gaps may arise, leading to inconsistencies in security measures.

Adebola Folorunso et al. [1] highlight the importance of "process transparency," where regular documentation of security measures and test results not only strengthens project credibility but also facilitates rapid incident response, such as in cases of critical vulnerabilities or data breaches.

It is crucial not only to formally define these procedures but also to ensure their enforcement. Companies implement training programs for specialists (QA engineers, DevOps teams, business analysts, etc.) to ensure that each participant understands their responsibilities [15].

Compliance should not become a mere "checkbox exercise" but should foster a mature security culture [7, 9]. Research by Stevens R. et al. [6] underscores that organizations treating cybersecurity as a purely formal requirement often discover vulnerabilities during testing. In contrast, an adaptive model integrates regulatory mandates into all testing scenarios, focusing on risk assessment and the specific characteristics of each information system [1].

Thus, testers and technical specialists align testing procedures to cover:

- Application architecture vulnerabilities.
- Data protection mechanisms during transmission and storage.
- Weaknesses in authentication and authorization.
- Conditions for storing and using log files.

Table 1 below presents examples of how different cybersecurity principles influence testing strategies.

Table 1. An example of the influence of various cybersecurity principles on the testing strategy (compiled by the author based on [1, 6, 13])

Regulator/Standard	Key Security Requirements	Impact on Testing Strategy
GDPR	Personal data protection, breach notification, right to data deletion	Testing personal data processing (including anonymization), verifying correct data deletion/update, auditing logs for compliance with confidentiality requirements
HIPAA	Security of medical information, confidentiality, accountability	Modeling PHI (Protected Health Information) leak scenarios, encryption verification, access rights audit for patient data, testing emergency shutdown procedures

Regulator/Standard	Key Security Requirements	Impact on Testing Strategy
PCI DSS	Payment data protection, network segmentation, transaction monitoring	Stress testing under high loads, encryption verification, card data storage checks, transaction log analysis, firewall and intrusion detection testing
ISO/IEC 27001	Comprehensive security management, continuous process improvement	Developing an audit system for testing, regular penetration testing, documenting incident management policies, integrating a risk-based approach
NIST Cybersecurity Framework	Identification, protection, detection, response, recovery	Threat modeling, response plan development, resilience analysis under failures, CI/CD tools application for continuous security monitoring

As seen in Table 1, different standards and regulatory frameworks impose specific security requirements, directly impacting the set of testing scenarios. Incorporating relevant checks for data protection, resource availability, and incident response mechanisms enhances the overall cyber resilience of a product.

Thus, cybersecurity principles serve as a foundational framework in test planning and execution, defining priorities and verification processes. This approach reduces the risk of overlooking critical vulnerabilities while enabling timely adaptation of testing methodologies to new regulatory requirements or architectural changes. The result is a robust strategy where security is not treated as a secondary factor but becomes an integral part of every stage of the testing process.

Key cybersecurity principles in testing

The core cybersecurity principles applied during testing enable a systematic approach to identifying and mitigating vulnerabilities before a product or system is deployed. Three fundamental areas are examined below: the risk-based approach and the confidentiality-integrity-availability (CIA) triad.

The risk-based approach in testing acknowledges that not all vulnerabilities have equal significance [8, 11]. Before initiating testing procedures, the following steps should be conducted:

- Threat Modeling: Analyzing potential entry points for attackers and identifying common attack scenarios (e.g., SQL injection, XSS).
- Risk Prioritization: Evaluating threats based on their potential impact (financial, reputational, legal) and likelihood of occurrence.

By identifying vulnerable code areas or modules handling sensitive information, testers can allocate the most effort and resources to these critical components [1]. For example, processing payment data under PCI DSS has a higher priority than testing auxiliary interfaces handling less sensitive information [5, 11].

Adebola Folorunso et al. [1] emphasize that a risk-based approach should not be a one-time procedure at the project's inception. Instead, it requires continuous reassessment as new requirements emerge, system architecture evolves, or data migrates to the cloud. Specifically:

- Risk Reviews and Updates: Conducted at iteration or sprint boundaries (in Agile/Scrum) or after major updates.
- Developer Feedback Loop: If a critical vulnerability is discovered during testing, the risk profile is adjusted based on new findings.

This dynamic adaptation significantly enhances the real-world security of the product [10].

Confidentiality and Protection of Test Data. In industries such as finance, healthcare, and government,

regulations impose strict data processing and storage requirements. For instance, GDPR mandates the anonymization or pseudonymization of personal information during testing [7, 13]. It is essential to ensure:

- Access control to the test environment, restricting test engineers from using real or near-real datasets.
- Encryption of test data during transmission and storage, both at the database level and in backup systems.

Additionally, HIPAA mandates that any operations involving personal medical data (PHI – Protected Health Information) must be logged and available for auditing [14]. Misconfigurations in the test environment that do not comply with HIPAA can result in severe legal consequences.

Integrity ensures that data remains unaltered (or is modified only through authorized actions) during testing [6, 15]. In practice:

- Hash values and checkpoints are used to validate data consistency before and after test execution.
- Continuous integration (CI/CD) processes incorporate static and dynamic code analysis tools (SAST, DAST) to detect integrity violations or unauthorized configuration changes [13].

Availability guarantees that users can access the system or data when needed. Testing plans often include:

- Load testing to assess system performance under peak traffic conditions.
- Failover testing to verify that system failures in one component do not disrupt the entire service [12, 14].
- Disaster recovery drills to evaluate recovery time and process efficiency for critical services [11, 13].

Table 2 below describes how the CIA triad principles are applied in test scenarios.

Table 2. Application of the CIA triad in test scenarios (compiled by the author, based on [1, 6, 11])

Principle	Key Measures	Example Test Scenarios
Confidentiality	- Data anonymization/pseudonymization - Encryption at rest and in transit - Role-based access control	1. Replacing test data to exclude personal identifiers for QA engineers. 2. Verifying TLS/SSL certificates and encryption mechanisms. 3. Ensuring only authorized personnel have access to sensitive data.
Integrity	- Version control and hash validation - Configuration management - Static and dynamic code analysis	1. Comparing hash values before and after database modifications. 2. Running SAST/DAST tools to detect insecure code injections. 3. Testing rollback procedures for faulty patch installations.
Availability	- Load and stress testing - Failover and disaster recovery tests - Resource consumption monitoring	1. Simulating peak traffic to measure response time (Load Testing). 2. Shutting down a server in a cluster to validate automatic failover. 3. Analyzing logs during unusual spikes in resource usage (DoS attack scenarios).

Ensuring compliance with the three core cybersecurity principles—risk-based testing, confidentiality-integrity-availability (CIA), and incident response readiness—is critical for comprehensive and effective testing procedures. Integrating these principles into testing methodologies allows organizations not only to meet

regulatory requirements but also to establish a genuine "security culture," where every identified deviation serves as a signal for continuous improvement.

Integration of automation and modern technologies in testing processes and cybersecurity principles

A common issue in compliance processes is the high volume of manual, repetitive checks and formal documentation. Automation tools enable:

- Real-time aggregation of testing metrics, including test results, logs, and vulnerability statistics.
- Generation of compliance reports aligned with specific regulatory standards (e.g., GDPR or PCI DSS), simplifying audits and certification processes [7, 4].
- Continuous compliance monitoring, providing timely alerts about potential misconfigurations in system settings [10].

As part of the DevOps approach, many organizations integrate specialized plugins and scripts into CI/CD (Continuous Integration / Continuous Delivery) pipelines to automatically verify security configurations at every stage of code deployment [6]. This helps detect configuration drift, a scenario where originally secure system settings deviate from compliance standards over time.

Another approach involves Robotic Process Automation (RPA)—software robots that simulate user actions or system requests. RPA robots can:

- Automatically compare actual server parameters, network rules, and account settings with baseline security values.
- Generate daily compliance reports and send them to SIEM systems or compliance officers for review [4, 9].

This significantly reduces the workload for testers and analysts, allowing them to focus on complex tasks such as developing new testing scenarios rather than performing manual documentation.

Machine learning (ML) algorithms enhance testing processes by enabling early detection of anomalies that may indicate new attack vectors [3, 9]. ML models can analyze:

- Application behavior under load, identifying unusual delays or errors.
- Network traffic in test environments to detect suspicious patterns, such as multiple authentication attempts from different IP addresses.
- Event logs (system, server, application), automatically prioritizing incidents based on their criticality.

Additionally, deep learning techniques help identify potential code vulnerabilities by analyzing extensive datasets of past incidents and patches, reducing the risk of human error [8].

Some AI-powered tools can automatically generate test scenarios based on functional descriptions and compliance requirements. For example, if GDPR requirements are specified, an ML module can identify relevant test steps, such as verifying data anonymization or enforcing the "right to be forgotten" [7]. Similarly, when HIPAA compliance is required, the system can automatically strengthen encryption checks for medical data.

A key advantage of AI solutions is their ability to adapt to emerging vulnerabilities and exploits. If new records appear in reference databases such as CVE (Common Vulnerabilities and Exposures), the tool updates corresponding test scenarios accordingly [1].

Integrating CI/CD with containerization allows security settings to be tested at every stage of image builds. For instance, Software Composition Analysis (SCA) can automatically check library versions for known vulnerabilities, ensuring compliance with PCI DSS or ISO/IEC 27001 component update requirements [5, 6].

Table 3 provides an overview of automation tools commonly used in testing, along with their functionalities.

Table 3. Example of automation tools used in testing, indicating their functions (compiled by the author based on [1, 3, 4])

Tool	Primary Functionality	Compliance Application
SAST/DAST (e.g., SonarQube, OWASP	Static and dynamic code analysis,	Identifies coding and exploitation risks relevant to PCI DSS, HIPAA, GDPR, etc.

Tool	Primary Functionality	Compliance Application
ZAP)	vulnerability detection	
SIEM Systems (e.g., Splunk, QRadar)	Security event log collection and correlation, anomaly detection	Automatic generation of compliance reports (ISO/IEC 27001), real-time alerting for security incidents
RPA (e.g., UiPath, Automation Anywhere)	Emulation of user/system actions, integration with external services	Automates routine comparisons of actual system parameters with baseline settings for audit and regulatory compliance
ML Platforms (e.g., TensorFlow, PyTorch with log analysis modules)	Training on historical data, behavior prediction, anomaly detection	Early detection of potential leaks or attacks, proactive alerts, and intelligent test case generation
SCA (Software Composition Analysis) (e.g., Snyk, WhiteSource)	Dependency and library vulnerability scanning	Ensures regular component updates to comply with PCI DSS and ISO/IEC 27001, streamlining compliance audit preparation

The integration of automation in testing processes enhances efficiency in identifying compliance deviations and improves security oversight. The use of AI and cloud technologies further strengthens this approach by enabling flexible scalability and intelligent diagnostics. These advancements contribute to the formation of a continuous improvement cycle, where every detected deviation from security standards becomes a driver for refining testing strategies and increasing compliance levels.

CONCLUSION

The study has substantiated that in modern conditions, the level of software security is largely determined by the extent to which cybersecurity principles are deeply and comprehensively integrated into the testing process. Merely adhering to regulatory requirements without considering the specifics of the testing environment and the risks associated with human factors can lead to missed critical vulnerabilities and inefficient resource allocation. In contrast, an integrated approach, where security requirements are embedded into test scenarios and methodologies, ensures a high level of protection and readiness to respond to incidents.

Key aspects of such integration include a risk-based approach to test design, the implementation of confidentiality, integrity, and availability (CIA triad) principles, and a proactive incident management strategy. Automation using CI/CD, SIEM, SAST/DAST tools, and machine learning algorithms facilitates timely detection of anomalies and simplifies compliance auditing. The examined examples demonstrate that only continuous improvement of internal security policies and regular risk assessments can maintain an adequate level of cyber resilience.

REFERENCES

Folorunso A. et al. Security compliance and its implication for cybersecurity //World Journal of Advanced Research and Reviews. – 2024. – Vol. 24 (1). – pp. 2105-2121.

Number of Cyberattacks Increases by 46 % in 2024. [Electronic resource] Access mode: https://coinspaidmedia.com/news/cyberattacks-increase-46-2024 / (date of access: 02/20/2025).

Machireddy J. R., Rachakatla S. K., Ravichandran P. Leveraging AI and machine learning for data-driven business strategy: a comprehensive framework for analytics integration //African Journal of Artificial Intelligence and Sustainable Development. – 2021. – Vol. 1 (2). – pp. 12-150.

Mohamed S. A. et al. Improving efficiency and effectiveness of robotic process automation in human resource management //Sustainability. – 2022. – Vol. 14 (7). – pp. 3920.

Carter W. A., Crumpler W. D. Financial Sector Cybersecurity Requirements in the Asia-Pacific Region. – Center for Strategic and International Studies (CSIS). - 2022. – pp.3-38.

Stevens R. et al. Compliance Cautions: Investigating Security Issues Associated with US Digital-Security Standards //NDSS. – 2020. – pp.2-10.

Taherdoost H. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview //Electronics. – 2022. – Vol. 11 (14). – pp. 2181.

Zografopoulos I. et al. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies //IEEe Access. – 2021. – Vol. 9. – pp. 29775-29818.

Huising R., Silbey S. S. Accountability infrastructures: Pragmatic compliance inside organizations //Regulation & Governance. – 2021. – Vol. 15. – pp. 40-62.

Marotta A., Madnick S. Convergence and divergence of regulatory compliance and cybersecurity //Issues in Information Systems. – 2021. – Vol. 22 (1). – pp. 10-50.

Hamdani S. W. A. et al. Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons //ACM Computing Surveys (CSUR). – 2021. – Vol. 54 (3). – pp. 1-36.

Nazarova K. et al. Preventional audit: implementation of SOX control to prevent fraud //Business: Theory and Practice. – 2020. – Vol. 21 (1). – pp. 293-301.

Williams B., Adamson J. PCI Compliance: Understand and implement effective PCI data security standard compliance. – CRC Press. - 2022.

Kaplan B. Phi protection under hipaa: An overall analysis //Kaplan, B.(with appendix by Monteiro, APL)," PHI Protection under HIPAA: An Overall Analysis," LGPD na Saúde (LGPD Applicable to Health), Dallari, AB, Monaco, GFC, ed., São Paulo: Editora Revista dos Tribunais (Thomsom Reuters). – 2020. – Vol. 2021. – pp. 61-88.

Alshaikh M., Adamson B. From awareness to influence: toward a model for improving employees' security behaviour //Personal and Ubiquitous Computing. – 2021. – Vol. 25 (5). – pp. 829-841