Journal of Mathematics Instruction, Social Research and Opinion
Vol. 5, No. 3, September 2026, pp. 2441 – 2453, https://doi.org/10.58421/misro.v5i3.1927
ISSN 2962-7842

Development and Functional Validation of a Quick Response Code-Based Archive Search and Tracking System for Digital Archive Management

Azhar Aulia Rahman[1], Metta Mariam[2]
[1,2]Informatics and Computer Engineering Education Study Program, Institut Prima Bangsa, Cirebon, Indonesia

Article Info

Article history:
Received 2026-07-16
Revised 2026-08-10
Accepted 2026-08-20

Keywords:
Archive Tracking
Black-Box Testing
Digital Archive Management
Functional Validation
Quick Response Code

ABSTRACT

Digital archive management requires rapid retrieval, visible archive status and location, controlled access, and traceable workflow decisions. Previous document-tracking studies have used code-based identifiers, but transparent functional validation of integrated archive workflows remains limited. This study developed and functionally validated a Quick Response Code-based archive search and tracking system for BPS Kota Cirebon. An applied software-development design with iterative prototyping was used. Thirty requirements-based black-box cases were executed on 24-25 July 2026 using synthetic records, one administrator account, one regular-user account, a Windows computer, and an Android device on the same local network. The initial test produced 24 passes and six failures involving attachment storage, approval processing, mobile code access, notifications, audit logging, and PDF export. After targeted corrections, all six cases passed on retest, yielding 30 final passes and a 100.0% defect-resolution rate. The study contributes a traceable functional-validation approach that connects identified defects, corrective actions, and retest evidence across integrated archive workflows. The tested build met all specified functional scenarios, while actual gains in retrieval time and employee workload require field evaluation.

Corresponding Author:
Azhar Aulia Rahman
Informatics and Computer Engineering Education Study Program, Institut Prima Bangsa, Cirebon, Indonesia
Email: azharaulrahman@gmail.com

1. INTRODUCTION

Archives provide evidence of organizational activity and support administrative accountability. Indonesian Law Number 43 of 2009 requires archival administration to maintain authenticity, integrity, reliability, and accessibility [1]. As public-sector organizations digitize records, effective archival systems must do more than store files: they must support retrieval, identify current status and location, control sensitive actions, and retain evidence of changes and access [2]–[4]. Indonesian studies likewise show that

electronic storage improves access only when classification, infrastructure, staff capability, and retrieval procedures are managed consistently [5]–[8].

Quick Response Codes can shorten the path from physical files to digital records, and prior studies have combined mobile access, code-based identifiers, and web workflows for document tracking [9], [10]. Yet the symbol itself only encodes a target; authorization, protected routes, histories, and audit records remain application-level responsibilities [11], [12]. Research on recordkeeping and archive services further emphasizes that technology must be accompanied by clear responsibilities, preservation practices, and accountability controls [13]–[21].

Two gaps follow. First, prior archive studies often discuss organizational adoption or present a completed application without documenting how functional failures were identified and resolved. Second, Quick Response Code-based tracking studies provide limited evidence of integrated validation across archive creation, metadata search, status and location tracking, role-based approval, notifications, protected downloads, audit logging, and reporting. This leaves uncertainty about whether interconnected functions behave as expected under valid, invalid, and unauthorized inputs.

Accordingly, this study aims to develop and functionally validate a Quick Response Code-based archive search and tracking prototype for BPS Kota Cirebon. Its originality lies not in code use alone, but in integrating physical-to-digital identification with centralized search, recorded status and location histories, controlled workflows, notifications, protected downloads, audit records, and report export, while preserving the engineering sequence from failure to correction and retest. The study asks: (1) do the implemented functions produce the expected observable results under the tested valid, invalid, and unauthorized conditions, and (2) what corrections are required when a function fails?

The study contributes a traceable functional-validation account that links requirements, defects, corrective actions, and retest evidence. Practically, the prototype is designed to reduce unnecessary search and confirmation steps and improve visibility of archive state and responsibility. Efficiency is therefore treated as a design objective and functional implication, not as a directly measured organizational outcome. Retrieval time, workload, user acceptance, concurrent performance, penetration security, and ISO/IEC 25010 conformity were outside the evaluation scope.

2. METHOD

2.1. Research Design and Context

This applied software-development study used iterative prototyping [22]. Each requirement was implemented as an interface or workflow, checked through a corresponding functional scenario, corrected when a defect was observed, and retested against the same objective. The prototype was developed for the archival workflow context of BPS Kota Cirebon. Functional testing was conducted on 24-25 July 2026 in a local development environment using a Windows computer and an Android device connected to the same network. The evaluation did not represent production deployment.

2.2. Test Units and Functional Scope

No human respondents or statistical population were involved. The units of analysis were implemented functions and their observable outputs. Thirty black-box cases were selected through requirements-based functional coverage rather than statistical sampling. The cases represented specified functions, access conditions, input categories, and workflow decisions across the six areas shown in Table 1.The functional requirements were derived from the specified prototype workflow, covering authentication and access, archive creation and requests, search and QR access, status and history, edit requests and notifications, and audit and reporting.

Table 1. Functional scope and black-box test coverage

Area	Main functions	Actors	Test cases
Authentication and access	Login, logout, protected routes, user management, and role restrictions	Administrator and user	BB-01–BB-08
Archive creation and requests	Direct archive entry, input validation, file upload, approval, and rejection	Administrator and user	BB-09–BB-14
Search and code access	Exact and partial search, unknown targets, mobile opening, and scan readability	Administrator and user	BB-15–BB-20
Status and history	Authorized status update, chronological history, and denied status changes	Administrator and user	BB-21–BB-23
Edit requests and notifications	Submission, approval, rejection, metadata update, and user notification	Administrator and user	BB-24–BB-27
Audit and reporting	Protected downloads, audit records, report creation, and export	Administrator and user	BB-28–BB-30

Digital archive management efficiency was operationalized as a design objective represented by five capabilities: direct Quick Response Code access from physical files to digital records, metadata search, visibility of current status and location, recorded approval and change histories, and notifications and audit records that reduce repeated manual confirmation. These capabilities were assessed for functional conformity; no before-and-after measurement of retrieval time, workflow steps, workload, cost, or coordination errors was performed.

The 30 cases therefore provide requirements-based functional coverage rather than exhaustive verification of every input combination, network condition, user configuration, or system path.

2.3. Data Sources and Test Environment

Primary data were the observable outcomes of the 30 executions, including interface responses, stored-data changes, access-control outcomes, generated files, notifications, audit entries, and Pass or Fail decisions. Synthetic records were used for archive metadata, files, requests, histories, notifications, audit records, and reports; confidential operational archives and personal data were not processed. Table 2 summarizes the test environment.

Table 2. Functional test environment

Component	Configuration
Application	Web prototype built with Laravel 12 and PHP 8.2.12
Database	MySQL/MariaDB in the local XAMPP development environment
Desktop client	Google Chrome on Windows 11
Mobile client	Android browser connected to the same local network
Server access	Local loopback address and a host address reachable on the same network, port 8001
Roles	One administrator account and one regular-user account
Test data and dates	Synthetic archive and workflow records; 24–25 July 2026

One administrator account and one regular-user account were used as system-testing accounts, not research participants. The web prototype used Laravel 12 and PHP 8.2.12 with MySQL/MariaDB in XAMPP; desktop access used Google Chrome on Windows 11, and mobile access used an Android browser on the same local network.

2.4. Research Instrument, Testing Procedure, and Trustworthiness

The instrument was a structured black-box matrix recording test ID, functional area, actor, precondition, action or input, expected result, observed result, supporting evidence, initial decision, and final retest decision. Black-box testing was selected because the evaluation concerned observable behavior rather than internal code coverage and is suitable for input validation, access restrictions, workflows, and generated outputs [23]–[27].

A case passed only when both the displayed response and resulting data matched the predetermined expectation. It failed if processing stopped, output was incorrect, a required data change was missing, or a prohibited action was allowed. Failed cases were diagnosed, corrected, and rerun against the same functional objective. Because no questionnaire or measurement scale was used, psychometric validity and reliability were not applicable; predetermined expectations, explicit decision rules, recorded evidence, and consistent retesting supported trustworthiness. Appendix A summarizes all cases.

2.5. Data Analysis and Ethical Considerations

Results were analyzed descriptively using the initial pass rate (PR) and defect-resolution rate (DR):

$$PR = (N_{pass} / N_{total}) \times 100\% \quad (1)$$

where Npass is the number of initial passes, and Ntotal is the total number of executed cases.

$$DR = (N_{resolved} / N_{failed}) \times 100\% \quad (2)$$

where Nresolved is the number of initially failed cases that passed after correction, and Nfailed is the number of initial failures.

Initial and final results were reported separately, and each failed case was analyzed by observed problem, technical cause, correction, and retest outcome. The study involved no human participants, interviews, or personal-data collection, so informed-consent procedures were not applicable. All test records were synthetic, testing remained in a local development environment, and identifying information in publication evidence was masked where necessary.

3. RESULTS

3.1. Prototype and Overall Functional Results

This section reports the implemented prototype, overall test outcomes, corrected failures, and remaining non-blocking findings. The prototype stores each archive under a tracking code and Quick Response Code and supports metadata search, role-based archive and request workflows, status and location histories, notifications, protected downloads, audit records, and report export.

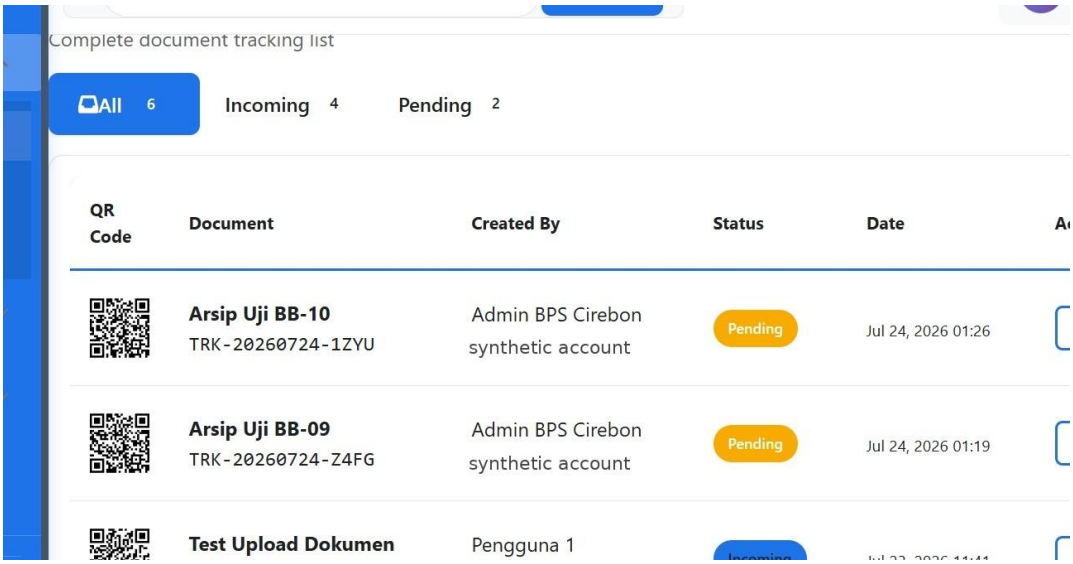

Figure 1. Archive master list with Quick Response Code identifiers and status information

A mobile-access check initially exposed a loopback target. After the target was changed to a host reachable on the same local network and the code was regenerated, the Android device opened the intended archive detail page (Figure 2).

Figure 2. Archive detail opened from an Android device on the same local network

The initial execution produced 24 passes and six failures, an 80.0% initial pass rate. After targeted corrections, all six failed cases passed on retest, giving 30 final passes and a 100.0% defect-resolution rate. Table 3 reports initial, retest, and final status separately so the correction history remains visible.

Table 3. Summary of black-box results

Cycle	Pass	Fail	Pass rate
Initial execution	24	6	80.0%
Retest of corrected cases	6	0	100.0% resolved
Final status after correction	30	0	100.0% of specified cases

Most specified functions therefore worked in the initial build, while six required correction before meeting their expected outcomes.

3.2. Defects, Corrections, and Retest Evidence

The six failures affected attachment-field mapping (BB-09), approval-to-archive conversion (BB-13), network reachability of the encoded target (BB-18), notification integration (BB-27), protected-download logging (BB-28), and PDF generation (BB-30). Table 4 records each observed failure, identified cause, correction, and retest result.

Table 4. Initial failures, corrective actions, and retest results

ID	Initial failure	Cause identified	Correction applied	Retest result
BB-09	A valid archive upload did not persist its attachment.	The controller used field names that did not match the attachment table.	The attachment fields used by the controller were aligned with the actual database columns, and the upload process was executed again.	The archive, attachment, tracking code, and QR Code image appeared in the master list: Pass.
BB-13	Approval changed the request status but did not create an active archive, attachment, and code.	The approval method stopped after updating the request status.	The method was revised to create the tracking record, attachment record, copied file, and code within one database transaction.	The approved request produced a traceable active archive: Pass.
BB-18	A valid code opened a loopback address that the Android device could not reach.	The generated target depended on localhost configuration.	The loopback target was replaced with a same-network host; the code was regenerated, and the front-end assets were rebuilt.	The Android device opened the intended archive detail page: Pass.
BB-27	An edit-request decision was not displayed as a user notification.	The controller, notification service, storage, and opening route were not fully connected.	Notification creation, database storage, route handling, and dropdown rendering were connected to the decision workflow.	The rejection title, document, and reason were displayed: Pass.
BB-28	Quick Response Code and attachment downloads were absent from the audit log.	The middleware did not record the relevant protected GET downloads.	Explicit audit-record creation was added to the protected code and attachment download handlers.	Both download types appeared with actor, action, model, description, address, and time: Pass.
BB-30	The Portable Document Format button simulated success, while the controller exported only comma-separated values.	The interface and route were not connected to a PDF-producing backend.	A DOMPDF view, format parameter, PDF controller branch, and report-specific export link were added.	A readable three-page PDF was downloaded and opened: Pass.

Three patterns were especially consequential. BB-13 required a single database transaction, so an approved request could not remain without its archive, attachment, tracking record, and code. BB-18 showed that a readable Quick Response Code can still fail when its target is unreachable from the scanning device. BB-28 and BB-30 required explicit integration of audit logging and PDF generation.

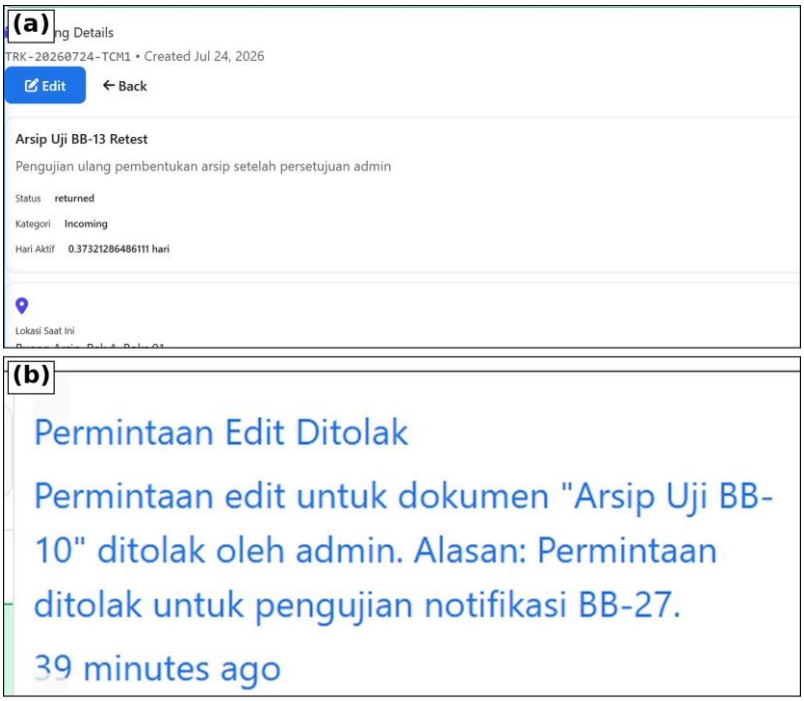

Figure 3. Retest evidence for workflow changes: (a) updated archive status and physical location; (b) rejection notification with the recorded reason

Figure 3 documents workflow and notification retests. During report retesting, the database contained seven documents and two pending records, which were reflected in the readable three-page PDF. Figure 4 documents protected-download audit entries and the generated report.

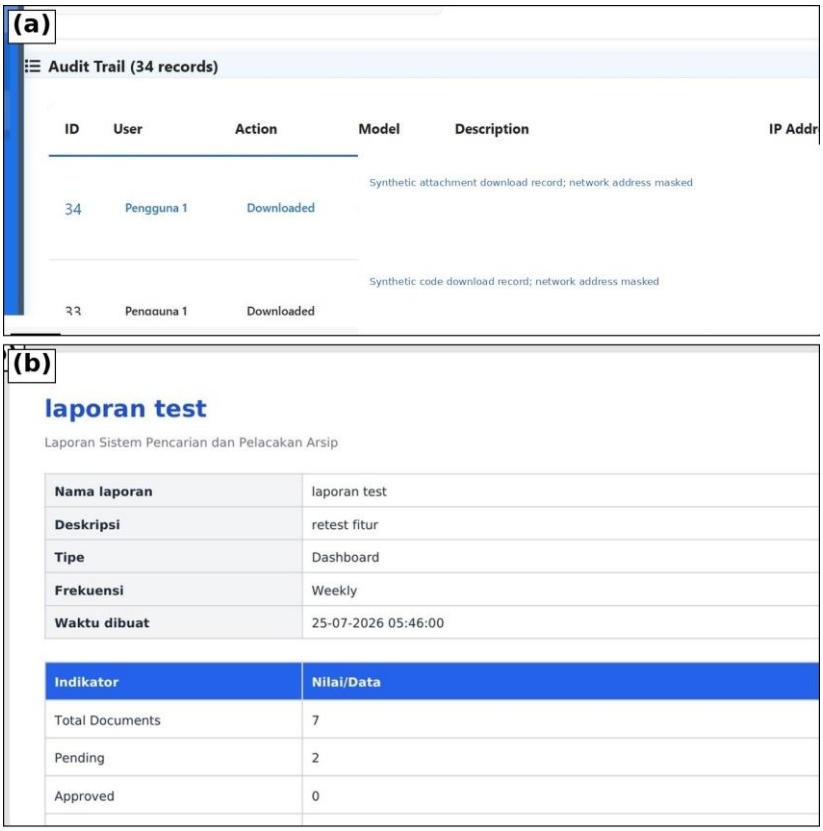

Figure 4. Retest evidence for traceability outputs: (a) protected-download entries in the audit log; (b) generated Portable Document Format report

3.3. Additional Coverage and Remaining Findings

The remaining 24 cases passed initially and covered authentication and session handling, user creation and duplicate validation, role restrictions, archive-input validation, request submission and rejection, exact and partial search, unknown tracking targets, partially covered codes, status and history operations, metadata-change decisions, and unauthenticated file access. Appendix A provides the complete matrix.

Three non-blocking findings remained after functional retesting: duplicated success feedback after rejection (UI-02), a generic not-found response for unknown tracking codes (UI-03), and locale-related CSV readability limits (UI-04). They did not change stored outcomes but may affect clarity or convenience (Table 5).

Table 5. Remaining non-blocking findings

Code	Finding	Effect	Recommended action
UI-02	A rejection action can display a duplicated success message.	The decision is stored correctly, but the feedback is repetitive.	Render one authoritative flash message for each completed action.
UI-03	An unknown tracking code shows a generic page-not-found response.	No unrelated record is displayed, but the message is not specific to archive lookup.	Provide a dedicated “tracking code not found” response.
UI-04	A comma-separated export opens in one Excel column under an Indonesian regional delimiter, and nested data appear as raw JSON.	The data are present, but spreadsheet readability is limited.	Use a locale-aware delimiter or a structured spreadsheet export; retain PDF for readable reports.

Overall, all 30 specified cases reached Pass after correction, while these three interface or compatibility issues remained outside the blocking functional criteria.

4. DISCUSSION

4.1. Interpretation and Comparison with Previous Studies

The principal finding is that functional conformity was achieved only after six defects across interconnected workflows were corrected. The initial 80.0% pass rate shows that 24 of the 30 specified functional cases met their expected outcomes before correction, while the correction history reveals where interface availability did not guarantee complete processing.

Previous studies show that Quick Response Codes, mobile access, and web workflows can support document identification and tracking [9], [10]. This study extends that scope by validating code-based access together with role authorization, status and location histories, notifications, protected downloads, audit records, and reporting. Its academic contribution lies in providing an integrated, traceable functional-validation record linking requirements, defects, corrective actions, and retest evidence, rather than introducing a new theory or QR Code technology.

The findings also extend prior work on digital archive governance and recordkeeping [2], [3], [13], [18], and [20] by demonstrating how these principles can be operationalized through testable application controls and audit evidence.

4.2. Workflow Consistency and Recordkeeping Governance

BB-13 was the most important consistency failure: the interface could show approval without creating the records that evidenced it. Moving the request update, file copy, tracking record, attachment, and code generation into one database transaction aligned the displayed decision with stored evidence. This supports recordkeeping principles that emphasize integrity, accountability, and attributable actions [2], [3], [13], [18], [20].

More broadly, successful role restrictions, protected routes, histories, notifications, and audit entries show how application-level controls can operationalize differentiated responsibilities in archive workflows. These results demonstrate functional traceability within the tested scenarios, not complete security or institutional effectiveness.

4.3. Cross-Device Access and Unexpected Engineering Findings

BB-18 distinguished symbol readability from resource accessibility. The initial code was readable but encoded a loopback address, so cross-device access failed until a reachable host was used. This is consistent with document-tracking work that treats mobile access as part of the workflow rather than a property of the symbol itself [9], [10].

The other failures reveal integration risks: BB-09 and BB-13 involved data consistency, BB-27 workflow integration, BB-28 traceability, and BB-30 output integration. Together they show why integrated workflows must be tested end-to-end and why reporting failure-correction-retest sequences offer stronger evidence of prototype maturity than reporting a final pass percentage alone.

4.4. Practical Implications

For BPS Kota Cirebon, the verified capabilities provide an operational basis for more structured archive retrieval and workflow control. Quick Response Code access and metadata search may reduce repeated manual searching; status and location histories may reduce reliance on individual memory; role restrictions clarify authority; notifications communicate decisions; and audit records preserve evidence of protected-resource access.

These are functionally supported implications. They do not establish measured gains in retrieval time, workload, workflow steps, cost, or coordination errors.

4.5. Limitations and Future Research

Findings are limited to 30 specified cases, synthetic data, two system-testing roles, one development build, and local-network access. BB-19 used an unknown tracking route rather than a separately printed invalid code, and BB-29 examined unauthenticated direct-link access rather than all user-to-user authorization paths. Usability, user acceptance, retrieval time, workload, concurrent load, long-duration stability, organizational impact, penetration security, and ISO/IEC 25010 conformity were not tested.

Future work should evaluate the system with actual archive-management staff in a stable institutional environment, compare retrieval time and workflow measures before and after implementation, and examine usability, broader authorization scenarios, concurrent performance, deployment security, reliability, backup and recovery, and relevant ISO/IEC 25010 characteristics.

5. CONCLUSION

This study developed and functionally validated a Quick Response Code-based archive search and tracking prototype for BPS Kota Cirebon. It asked whether specified functions produced expected outputs under tested valid, invalid, and unauthorized conditions and what corrections were needed when they failed. The initial test identified six defects, and all 30 specified cases passed after targeted corrections. Within the tested scope, the implemented functions therefore achieved their expected observable outcomes after correction; the required fixes concerned data-field alignment, transactional workflow processing, network configuration, notification integration, audit recording, and PDF generation.

Academically, the study contributes evidence that Quick Response Code-based archive identification should be evaluated as part of an integrated governance workflow rather than as an isolated access mechanism. Its distinctive contribution is the traceable linkage of requirements, initial failures, technical causes, corrective actions, and retest evidence across archive search, tracking, authorization, notification, audit, and reporting functions.

Practically, the prototype provides a functional basis for structured archive retrieval, visible status and location information, controlled decisions, and attributable activities. The evidence does not quantify organizational efficiency and is limited to synthetic records, two test roles, one development build, and local-network testing.

Future studies should deploy the system in an operational environment with actual users and measure retrieval time, workflow steps, workload, usability, acceptance, concurrent performance, security, long-term reliability, and relevant ISO/IEC 25010 characteristics.

ACKNOWLEDGEMENTS

The authors thank BPS Kota Cirebon for providing the institutional context used to define the archive search and tracking workflow.

REFERENCES

[1] Republic of Indonesia, Law of the Republic of Indonesia Number 43 of 2009 concerning Archives. Republic of Indonesia, 2009. [Online]. Available: https://peraturan.bpk.go.id/Details/38788/uu-no-43-tahun-2009

[2] M. P. Damanik et al., "Digital Archives Management in the Public Sector: A Bibliometric Study," Khizanah Al-Hikmah J. Ilmu Perpustakaan, Informasi, dan Kearsipan, vol. 12, no. 2, pp. 304–318, 2024, doi: 10.24252/kah.v12i2a7.

[3] H. Bawono, "Digital Preservation and Digital Records and Archives Management in Indonesia: Contextualization-Synthesis of Two Models Digital Preservation," J. Kearsipan, vol. 17, no. 2, pp. 147–169, 2022, doi: 10.46836/jk.v17i2.257.

[4] K. R. Lee and K. S. Lee, "The Korean government's electronic record management reform: The promise and perils of digital democratization," Gov. Inf. Q., vol. 26, no. 3, pp. 525–535, 2009, doi: 10.1016/j.giq.2009.03.007.

[5] M. Rifauddin, "Pengelolaan arsip elektronik berbasis teknologi," Khizanah Al-Hikmah J. Ilmu Perpustakaan, Informasi, dan Kearsipan, vol. 4, no. 2, pp. 168–178, 2016, doi: 10.24252/kah.v4i27.

[6] D. A. Caroline, B. Ismanto, and L. Rina, "Implementation of digital archives using a dynamic archive information system," J. Kaji. Inf. Perpust., vol. 10, no. 2, pp. 189–204, 2022, doi: 10.24198/jkip.v10i2.33203.

[7] Yunita and E. Rahmah, "Penerapan arsip elektronik di Kantor Perpustakaan, Arsip, dan Dokumentasi Kota Bukittinggi," J. Ilmu Inf. Perpust. dan Kearsipan, vol. 4, no. 1, pp. 326–334, 2015, doi: 10.24036/6183-0934.

[8] F. Zuliyanti, "Pengolahan arsip dinamis inaktif sebagai upaya efektivitas dan efisiensi temu kembali arsip di BAPPEDA Kabupaten Bantul," Informatio J. Libr. Inf. Sci., vol. 1, no. 3, pp. 241–258, 2021, doi: 10.24198/inf.v1i3.35257.

[9] M. Alfiareza and N. Wilantika, "Sistem Pelacakan Dokumen Berbasis Seluler dan Kode QR," J. Teknol. Inf. dan Ilmu Komput., vol. 9, no. 3, pp. 453–462, 2022, doi: 10.25126/jtiik.2022924519.

[10] S. F. Salleh, H. Ujir, R. Sapawi, and H. F. Hashim, "Accreditation document tracking system using Scrum approach," Int. J. Eval. Res. Educ., vol. 9, no. 1, pp. 153–161, 2020, doi: 10.11591/ijere.v9i1.20418.

[11] ISO/IEC, "ISO/IEC 18004:2024, Information technology—Automatic identification and data capture techniques—QR code bar code symbology specification," International Organization for Standardization, Geneva, Switzerland, Aug. 2024. [Online]. Available: https://www.iso.org/standard/83389.html

[12] E. H. Rachmawanto, R. S. Gumelar, Q. Nabila, C. A. Sari, and R. R. Ali, "Testing Data Security Using a Vigenere Cipher Based on the QR Code," KINETIK, vol. 8, no. 4, pp. 701–708, 2023, doi: 10.22219/kinetik.v8i4.1734.

[13] H. Bawono, R. Darmagara, and R. A. Parikesit, "National movement for good recordkeeping awareness and commitment to archiving in Indonesia," J. Kaji. Inf. Perpust., vol. 10, no. 1, pp. 29–46, 2022, doi: 10.24198/jkip.v10i1.34644.

[14] F. Irmalasari and N. Mayesti, "Strategy of National Archives of the Republic of Indonesia in improving service quality: A case study of Sub Directorate of Archive Services," Rec. Libr. J., vol. 3, no. 2, pp. 158–171, 2017, doi: 10.20473/rlj.V3-I2.2017.158-171.

[15] N. Iswandi, N. A. Nazifah, H. Khotimah, M. Anggraini, and J. J. Okshi, "Sistem manajemen arsip di MTS Aulia Cendikia Palembang," Dipl. J. Kearsipan Terap., vol. 2, no. 2, pp. 65–74, 2019, doi: 10.22146/diplomatika.42038.

[16] S. Kartini, Sukaesih, and A. Budiono, "Kinerja pengelolaan arsip Kantor Pelayanan Utama Bea dan Cukai Tipe A Tanjung Priok," J. Kaji. Inf. Perpust., vol. 7, no. 2, pp. 175–190, 2019, doi: 10.24198/jkip.v7i2.21250.

[17] A. Kuswantoro and S. Hartati, “Pengaruh kompetensi pegawai dan sarana prasarana kearsipan terhadap pengelolaan arsip dinamis di kantor kelurahan se-Kecamatan Gunungpati Kota Semarang,” Khazanah J. Pengemb. Kearsipan, vol. 12, no. 2, pp. 171–185, 2019, doi: 10.22146/khazanah.48843.

[18] K. Stuart, “Methods, methodology and madness: Digital records management in the Australian government,” Rec. Manag. J., vol. 27, no. 2, pp. 223–232, 2017, doi: 10.1108/RMJ-05-2017-0012.

[19] F. Tjiptasari, “Persepsi kegunaan pengelolaan arsip digital menggunakan SIKD,” J. Kaji. Inf. Perpust., vol. 5, no. 2, pp. 111–126, 2017, doi: 10.24198/jkip.v5i2.12645.

[20] Q. Xiao, X. Xu, and P. Liu, “Security status of electronic records preservation in central China: The survey results of 34 archives in Wuhan City,” Libr. Hi Tech, vol. 39, no. 1, pp. 22–36, 2021, doi: 10.1108/LHT-04-2019-0088.

[21] Y. N. Ifriza and S. Sudarno, “Improving Dynamic Archive Security Based Biometric System for Identification and Authentication with Personal Fingerprint,” Econ. Educ. Anal. J., vol. 10, no. 3, pp. 477–486, 2021, doi: 10.15294/eeaj.v10i3.49877.

[22] R. S. Pressman and B. R. Maxim, Software Engineering: A Practitioner’s Approach, 9th ed. New York, NY, USA: McGraw-Hill, 2019.

[23] M. S. Mustaqbal, R. F. Firdaus, and H. Rahmadi, “Pengujian aplikasi menggunakan black box testing boundary value analysis (Studi Kasus: Aplikasi Prediksi Kelulusan SMNPTN),” J. Ilm. Teknol. Inf. Terap., vol. 1, no. 3, pp. 31–36, 2015, doi: 10.33197/jitter.vol1.iss3.2015.62.

[24] D. Ahrizal, M. K. Miftah, R. Kurniawan, T. Zaelani, and Y. Yulianti, “Pengujian perangkat lunak sistem informasi peminjaman PlayStation dengan teknik boundary value analysis menggunakan metode black box testing,” J. Inform. Univ. Pamulang, vol. 5, no. 1, pp. 73–77, 2020, doi: 10.32493/informatika.v5i1.4338.

[25] I. D. Kusuma, I. G. L. A. O. C. Pradipta, and U. L. Yuhana, “Black Box Testing in the Access by KAI Application Using Boundary Value Analysis and Graph-Based Testing,” INFOTECH J., vol. 10, no. 1, pp. 122–127, 2024, doi: 10.31949/infotech.v10i1.9577.

[26] F. D. Hartono and Y. Sugiarti, “Perbandingan metode equivalence partitions dan boundary value analysis pada pengujian black box: Literatur review,” Maj. Ilm. METHODA, vol. 12, no. 2, pp. 153–159, 2022, doi: 10.46880/methoda.Vol12No2.pp153-159.

[27] W. N. Cholifah, Yulianingsih, and S. M. Sagita, “Pengujian Black Box Testing pada Aplikasi Action & Strategy Berbasis Android dengan Teknologi Phonegap,” STRING Satuan Tulisan Ris. dan Inov. Teknol., vol. 3, no. 2, pp. 206–210, 2018, doi: 10.30998/string.v3i2.3048.

APPENDIX A. BLACK-BOX TEST MATRIX

Table A1 summarizes the 30 executed cases. Detailed causes and corrective actions for the six initial failures are reported in Table 4. An initial Fail followed by a final Pass indicates successful correction and retest.

Table A1. Summary of black-box results for BB-01–BB-30

ID	Scenario and expected result	Initial	Final
BB-01	Valid administrator login; dashboard and authenticated session created.	Pass	Pass
BB-02	Valid regular-user login; role-appropriate dashboard and menu displayed.	Pass	Pass
BB-03	Incorrect password rejected; no authenticated session created.	Pass	Pass
BB-04	Protected page opened without login; redirected and content withheld.	Pass	Pass
BB-05	Logout followed by protected URL reuse; session invalidated.	Pass	Pass
BB-06	Administrator adds a valid user; account saved and displayed.	Pass	Pass
BB-07	Duplicate user data submitted; validation rejects the record.	Pass	Pass
BB-08	Regular user opens user management; administrator data remains blocked.	Pass	Pass
BB-09	Valid archive upload; archive, attachment, tracking code, and code image created.	Fail	Pass
BB-10	Required archive metadata omitted; invalid record is not saved.	Pass	Pass
BB-11	Invalid file type uploaded; file rejected and application remains stable.	Pass	Pass
BB-12	Regular user submits archive request; pending request stored and visible.	Pass	Pass
BB-13	Administrator approves request; active archive, attachment, and code created.	Fail	Pass
BB-14	Administrator rejects request; reason stored and no active archive created.	Pass	Pass
BB-15	Exact-title search; correct archive returned.	Pass	Pass
BB-16	Partial-title or metadata search; relevant archive returned.	Pass	Pass
BB-17	Nonexistent search term; stable no-result response and no unrelated data.	Pass	Pass
BB-18	Valid code scanned; intended detail page opens on the Android device.	Fail	Pass
BB-19	Unknown tracking target; not-found response and no other archive exposed.	Pass	Pass
BB-20	Partially covered code; unreadable while covered and valid after uncovering.	Pass	Pass
BB-21	Authorized status update; new status saved and displayed.	Pass	Pass
BB-22	Status history reviewed; chronological actor and time information displayed.	Pass	Pass
BB-23	Unauthorized status update attempted; action denied and data unchanged.	Pass	Pass
BB-24	Regular user submits metadata-change request; pending request stored.	Pass	Pass
BB-25	Administrator approves metadata change; target data and decision updated.	Pass	Pass
BB-26	Administrator rejects metadata change; existing data retained and reason shown.	Pass	Pass
BB-27	Important decision issued; user notification and reason displayed.	Fail	Pass
BB-28	Protected code and attachment downloads; complete audit entries recorded.	Fail	Pass
BB-29	Protected file opened without authentication; redirected and file withheld.	Pass	Pass
BB-30	Report created; comma-separated values and readable PDF downloaded.	Fail	Pass