International Journal of Safety and Security Engineering
Vol. 16, No. 10, October, 2026, pp. 2411-2417
Journal homepage: http://iieta.org/journals/ijsse

A Multi-Case Pilot Study of a Three-Phase Security Governance Implementation in Software Startups

Doddy Ferdiansyah[1,2*], R. Rizal Isnanto[3], Jatmiko Endro Suseno[4]

[1] Doctoral Program in Information Systems, School of Postgraduate Studies, Universitas Diponegoro, Semarang 50241, Indonesia
[2] Department of Informatics Engineering, Universitas Pasundan, Bandung 40153, Indonesia
[3] Department of Computer Engineering, Universitas Diponegoro, Semarang 50275, Indonesia
[4] Department of Physics, Universitas Diponegoro, Semarang 50275, Indonesia

Corresponding Author Email: doddyferdiansyah@students.undip.ac.id

Copyright: ©2026 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.161017

Received: 6 September 2026
Revised: 14 October 2026
Accepted: 23 October 2026
Available online: 31 October 2026

Keywords:
key informant method, pilot study, Secure Software Development Lifecycle, security champion, security governance roadmap, software startups

ABSTRACT

Secure software development practices are rarely adopted in resource-constrained startups, and governance roadmaps derived from survey models have seldom been tested in practice. This study evaluates a three-phase security governance roadmap, derived from a six-factor model of Secure Software Development Lifecycle (SSDL) adoption, in a multi-case pilot. Using the key informant method, one senior respondent from each of four Indonesian software startups rated SSDL Adoption Effectiveness on a 1–5 scale before and after a nine-week implementation and completed a 17-item activity checklist, complemented by qualitative accounts of security-champion institutionalization. All four cases reported higher scores: the mean increase was 1.83 (standard deviation (SD) = 0.67; 95% Confidence Interval (CI) 0.77–2.88), paired $t(3) = 5.49$, $p = 0.0119$, Cohen's $d_z = 2.74$, and checklist completion rose from 7.0 to 15.5 of 17 items. Improvement appeared in all five effectiveness indicators, most strongly in documentation consistency and least in resource support. Three startups fully institutionalized a security champion role; one did so partially. With four cases, one self-reporting informant per case, and no control group, the findings are preliminary and describe perceived change. They suggest that the roadmap is feasible for small teams and provide a basis for larger, multi-informant evaluations.

1. INTRODUCTION

Software startups face a structural tension between shipping speed and the discipline that secure software development requires. Prior work in this research programme showed that startups possess little of the formal governance apparatus that secure development frameworks assume [1, 2], and a subsequent three-factor model explained a substantial share of the variance in Secure Software Development Lifecycle (SSDL) adoption effectiveness ($R^2 = 0.439$) [3]. A six-factor extension, estimated in authors' research on survey responses from 95 startup practitioners, identified security practice integration as the strongest direct predictor of adoption effectiveness, with security leadership acting only indirectly through it. That model was translated into a three-phase, contextual security governance roadmap for resource-constrained startups; its derivation is summarized in Section 2.1 and is not repeated here.

A statistically estimated model, and a roadmap derived from it, are not evidence that the roadmap works in practice. Frameworks written for well-resourced organizations routinely fail to translate into small teams unless adapted, sequenced, and actively supported [4-6]. The obstacle is rarely unawareness of good practice, but the absence of a realistic, staged path for adopting it with limited people and time [7-10]. A roadmap derived from cross-sectional survey data therefore leaves an open question: does it work when a real startup applies it?

The stakes of getting this right are practical as well as academic. Startups that under-invest in security governance face compounding technical debt and regulatory exposure as they scale, while those that over-invest risk diverting scarce engineering capacity away from product development at a stage when that capacity often determines survival. A roadmap that is associated with higher adoption effectiveness, even in a small pilot, without requiring the full apparatus of an enterprise security programme would therefore be relevant beyond the cases studied here.

This corresponds to the demonstration-and-evaluation stage of a design science research (DSR) programme [11]. The governance model and roadmap were designed and statistically estimated in the earlier study but have not yet been evaluated in the naturalistic, ex post sense of the Framework for Evaluation in Design Science Research (FEDS) [12]. This study fills that gap: it reports a multi-case pilot implementation of the three-phase roadmap in four software startups, using the

key informant method [13] to assess SSDL Adoption Effectiveness before and after implementation, together with informants' accounts of security-champion institutionalization.

A recurring mechanism for embedding security into small teams is the security champion, whose effectiveness depends on integration into daily workflow rather than on the role being merely named [14]. Champions are described as force multipliers for security behavior change [15], and sustained intervention, rather than one-off training, is what shifts developer security behavior [16]. Champions appointed without organizational support tend not to produce change [17], and a role that is not actively maintained and connected to routine practice atrophies [18]. This is consistent with the general literature on innovation champions [19], on frameworks for driving the adoption of software security practices [20], and on connecting developer practice to organizational controls [21]. Security culture, similarly, is cultivated rather than declared [22, 23]. Outside SSDL, phased adoption is a documented pattern for small organizations pursuing ISO/IEC 27001 [24-26]; however, none of this literature evaluates a roadmap derived from an empirically estimated mediation model through a key-informant pilot in the startup population, which is the gap addressed here.

This paper does not re-analyze the six-factor model; its contribution is the pilot implementation evidence itself: preliminary field evidence for the roadmap, obtained from real startups rather than further surveys; a qualitative account of security-champion institutionalization that provides process-level context for the mediation mechanism identified in the earlier survey model; and a demonstration that the key-informant method, applied to a small multi-case pilot, is workable for generating implementation evidence in populations that are difficult to sample at scale.

2. METHODOLOGY

2.1 Design and source model

This study is the demonstration-and-evaluation stage of a DSR programme [11]; the earlier stages were problem identification and design of the six-factor model and the three-phase roadmap. Evaluation follows FEDS [12], which distinguishes artificial from naturalistic and ex ante from ex post evaluation. This study is naturalistic and ex post: the roadmap was applied by real key informants inside their own organizations, after the artifact had already been designed. It is not a replication of the underlying structural model - four organizations are far below what structural equation modeling requires - but a small, case-based, mixed-methods design that combines quantitative pre-post self-assessment with qualitative accounts, in line with recommendations for triangulating quantitative organizational findings with qualitative case evidence [27]. Figure 1 summarizes the overall pilot workflow.

The source model from earlier research relates six governance factors to SSDL Adoption Effectiveness (Y). It was estimated with partial least squares structural equation modeling (PLS-SEM) on responses from 95 startup practitioners recruited through the same regional network. All indicator loadings exceeded 0.70, composite reliability ranged from 0.88 to 0.94, average variance extracted from 0.59 to 0.88, and the highest heterotrait-monotrait (HTMT) ratio was 0.83. The model explained 76.9% of the variance in Y. Security practice integration (X5) had the strongest direct path to Y ($\beta = 0.311$, $p = 0.003$). Security leadership (X6) had no significant direct effect on Y ($\beta = 0.114$, $p = 0.070$) but a significant effect on X5 ($\beta = 0.473$, $p < 0.001$) and a significant indirect effect on Y through X5 ($\beta = 0.147$, $p = 0.017$; variance accounted for = 56.3%), so X5 mediates the effect of X6. These estimates are used here only as the rationale for the roadmap.

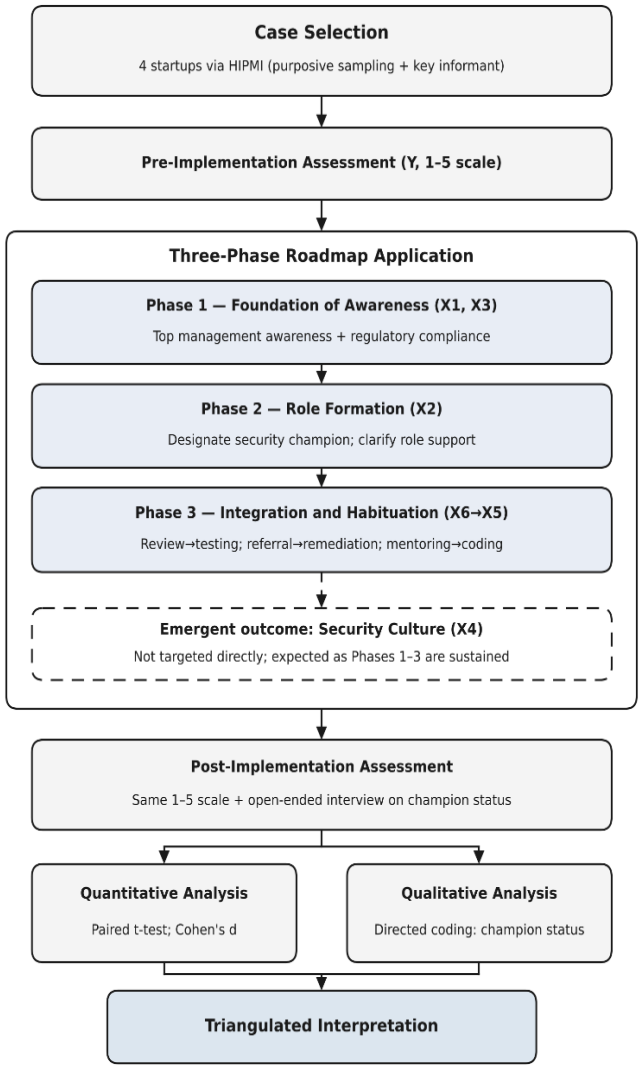


Figure 1. Overall pilot study flow

Table 1. Three-phase security governance roadmap

Phase	Targeted Factor(s)	Concrete Activities
1. Foundation of awareness	X1, X3	Brief management on SSDL risk and lifecycle; identify regulatory requirements
2. Role formation	X2	Designate a security champion; clarify role and management support
3. Integration and habituation	X6 into X5	Review→testing; issue referral→remediation; mentoring→coding standards
(Emergent outcome)	X4	Expected to develop as Phases 1-3 are sustained

Note: Secure Software Development Lifecycle (SSDL).

The roadmap operationalizes six governance factors (X1:

Top Management Awareness; X2: Security Team Availability; X3: Regulatory Compliance; X4: Security Culture; X5: Security Practice Integration; X6: Security Leadership) into three phases, following the path structure of the source model and consistent with staged-adoption logic for ISO/IEC 27001 in small organizations [24, 26]. Phase 1 builds a foundation of awareness (X1, X3); Phase 2 forms the security role, including designating a security champion (X2); Phase 3 integrates security leadership into daily practice (X6 into X5): security review is linked to routine testing, issue referral to rapid remediation, and mentoring to secure coding standards. Security culture (X4) is treated as an emergent outcome of Phases 1-3 rather than a separate phase. Table 1 summarizes the roadmap.

2.2 Participants and procedure

This study uses the key informant method: data were collected from a single respondent per organization judged, by position and breadth of involvement, to validly represent organizational-level conditions [13]. This is appropriate because the unit of analysis is organizational SSDL governance practice, and the participating startups are generally too small to support multiple independent informants without disrupting delivery work. Each key informant held a role with cross-functional SDLC visibility (Chief Technology Officer (CTO), Chief Executive Officer (CEO), or Tech Lead) and was close enough to day-to-day development decisions to speak to both the baseline and the changes observed.

Four software startups were recruited through the West Java network of the Indonesian Young Entrepreneurs Association (HIPMI), using purposive selection against three criteria: the organization develops software in-house; it committed to applying the roadmap over nine weeks (late May to late July 2026); and the key informant held a cross-functionally visible role. To protect confidentiality, no personal names are reported; each case is identified by the startup's short name and the informant's role.

The researcher held a single online briefing on 23 May 2026, from 20.00 to 21.30 WIB (90 minutes), to explain the purpose of the pilot and the activities each startup was to carry out; the informants completed the baseline assessment during this period. No further meetings were held. Until the post-implementation assessment (26–28 July 2026, about nine weeks later), the researcher only monitored the submitted responses and answered informants' questions when asked, and did not carry out activities in the organizations. Informants carried out the activities within their own organizations, and delivery differed across cases (Section 3.4). No fixed schedule was set for the three phases: each startup applied them at its own pace, and phase durations were not recorded. Informants recorded their assessments in a web-based application developed by the researcher, with an individual login for each informant.

2.3 Measures

SSDL Adoption Effectiveness (Y) was assessed with the same five-indicator instrument used in the source study (process efficiency, output quality and security, consistency of security implementation, resource support, and SSDL documentation consistency). Each indicator is the mean of two Likert items (ten items in total), and Y is the mean of the five indicators. Reusing this instrument preserved construct continuity and avoided introducing a new measure into a small-sample design. Each informant completed the instrument on a 1–5 scale before the roadmap was introduced and again after the nine weeks, supplemented by open-ended questions on security-champion designation and activity. Implementation was also recorded with a 17-item checklist. Each item corresponds to one of the indicators retained for X1-X5 in the final source model (X1: five; X2: four; X3: three; X4: two; X5: three) and was answered "done" or "not yet", with an optional free-text note. Items map to the roadmap as follows: X1 and X3 items to Phase 1 (eight items), X2 items to Phase 2 (four), X5 items to Phase 3 (three), and X4 items to the emergent outcome (two). The full checklist is provided in Table A1. Security leadership (X6) was not a checklist item and was covered by the open-ended questions. The checklist is a self-reported process measure and does not verify that an activity was completed.

2.4 Analysis

The aggregate change in Y was summarized with mean, standard deviation (SD), and 95% Confidence Interval (CI), and tested with a two-tailed paired-samples t-test. The effect size is Cohen's d_z, the mean difference divided by the SD of the paired differences, reported with Hedges' small-sample correction (g_z). Given n = 4, the consistency and magnitude of the effect across cases and the width of the interval are treated as more informative than the *p*-value alone [28]. The change in each of the five Y indicators is reported descriptively (mean change, range, and interval) and is not interpreted inferentially. Qualitative responses on security-champion institutionalization were coded, following recommended case-study practice [29], as fully, partially, or not institutionalized, based on whether the informant reported a named role holder, concrete activities, and integration into routine practice. Quantitative and qualitative results were then interpreted jointly as methodological triangulation [27].

3. RESULTS AND DISCUSSION

3.1 Case overview

Table 2 summarizes the four cases with pre- and post-implementation Y scores together with the number of checklist items reported as done (Appendix), collected alongside the Y instrument as a self-reported process measure.

Table 2. Case profiles and pre/post scores

Case	Role	Pre (Y)	Post (Y)	ΔY	Checklist Pre	Checklist Post
Etafilia	CTO	2.2	4.7	+2.5	3/17	14/17
Kunci	Tech Lead	3.8	4.8	+1.0	15/17	17/17
Pilar	CEO	2.7	4.9	+2.2	5/17	15/17
Anaheim	CEO	2.8	4.4	+1.6	5/17	16/17

Note: Chief Technology Officer (CTO); Chief Executive Officer (CEO); Secure Software Development Lifecycle (SSDL).

3.2 Aggregate quantitative result

All four cases reported a higher SSDL Adoption Effectiveness score after the roadmap was applied (Table 2).

The mean increase was $\Delta Y = 1.83$ (SD = 0.67; 95% CI 0.77–2.88), paired $t(3) = 5.49$, $p = 0.0119$, Cohen's $d_z = 2.74$ (Hedges' $g_z = 2.00$). The interval is wide, which reflects the four-case sample, and the *p*-value should be read as descriptive: with four pairs, an exact non-parametric test cannot fall below $p = 0.125$. More informative is that the direction of change was the same in all four cases (+1.0 to +2.5), and that cases starting from different baselines (Y = 2.2–3.8) ended in a similar, high post-implementation range (Y = 4.4–4.9). The smallest gain (Kunci, +1.0) came from the highest starting point (Y = 3.8; 15 of 17 checklist items already done), which leaves less room for improvement and should not be read as a weaker response. Checklist completion rose from a mean of 7.0 to 15.5 of 17 items, and no item that was done at baseline was reported as not done afterwards. Because the same informants supplied the checklist, this agreement shows internal consistency of self-reports and not independent corroboration (Section 3.6).

3.3 Per-dimension analysis

Table 3 and Figure 2 present the pre- and post-implementation profiles of the five Y indicators, with detailed case-level scores provided in Table A2. All five increased on average (+1.13 to +2.13).

Table 3. Change in the five Y indicators

Indicator	Pre	Post	Mean Δ	Range of Δ	95% CI of Δ
Y_P1 Efficiency	3.00	4.88	1.88	1.0–3.0	0.52 to 3.23
Y_P2 Quality, security	2.75	4.75	2.00	1.5–2.5	1.08 to 2.92
Y_P3 Consistency	2.75	4.75	2.00	1.5–2.5	1.08 to 2.92
Y_P4 Resources	3.13	4.25	1.13	0.5–2.0	−0.07 to 2.32
Y_P5 Documentation	2.75	4.88	2.13	0.5–3.0	0.36 to 3.89

Note: Values are rounded; change is computed from unrounded means. CI: 95% confidence interval of the mean change (n = 4). Confidence Interval (CI).

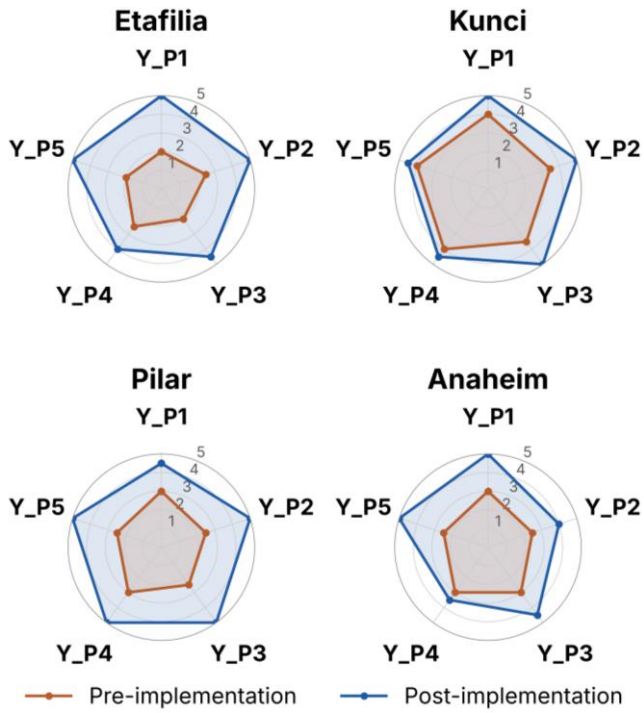


Figure 2. Pre- and post-implementation scores

The largest mean gains were in SSDL Documentation Consistency (Y_P5, +2.13), Output Quality and Security (Y_P2, +2.00), and Consistency of Security Implementation (Y_P3, +2.00); Process Efficiency (Y_P1) rose by 1.88 and Resource Support (Y_P4) by 1.13, the only indicator whose interval includes zero. Gains in Y_P5 varied most across cases (0.5 to 3.0). The four larger gains differ by no more than 0.25 points, which four cases cannot distinguish, so the pilot shows broad improvement and not a gain concentrated in indicators close to security practice integration. The weaker change in Y_P4 is plausible, since budget and staffing decisions lie largely outside a startup's governance actions within nine weeks, but this explanation was not tested.

3.4 Process fidelity and qualitative findings: Security champion institutionalization

Three of the four startups (Kunci, Pilar, Etafilia) fully institutionalized the security champion role, identifying a named role holder with concrete, recurring activities; Anaheim did so only partially (Table 4). At Etafilia, the champion role was absorbed into an existing senior technical position (the CTO), mapping directly onto the Phase 3 pairing of security review with routine testing; checklist completion moved from the lowest starting point among the four cases (3 of 17) to 14 of 17, a gain of 11 items, equal to that of Anaheim. At Kunci, secure coding and testing already existed; what the roadmap added was named accountability for security that had not previously existed - illustrating that the binding constraint in some organizations is not absent practice but an absent responsible role. At Pilar, the CTO was designated champion, security was discussed for each feature or application in a fixed weekly session, and the champion simply tested each completed feature while still learning security testing; findings went directly to the developers for repair.

Table 4. Security champion status by case

Case	Status	Note
Etafilia	Full	CTO took the role directly: reviewing completed features and monitoring team security activity.
Kunci	Full	Tech Lead designated the Director of Backend Development; testing already practiced, role newly formalized.
Pilar	Full	CTO designated as champion; weekly security discussion; simple test of each completed feature.
Anaheim	Partial	Role assigned to the CTO; testing still done by programmers; testing and documentation ownership unresolved at pilot end.

Note: Chief Technology Officer (CTO).

Pilar and Anaheim began from an identical checklist baseline (5 of 17 items) and reached a similar level of overall

activity completion by the end of the pilot (15 of 17 and 16 of 17, respectively), yet their qualitative outcomes diverged: Pilar fully institutionalized the champion role and connected it to routine development activity, while Anaheim's role assignment remained incomplete in practice: the role was given to the CTO, but testing was still done by the programmers. This divergence, despite near-identical aggregate checklist completion, indicates that overall activity completion and the specific relational outcome Phases 2 and 3 target—a role that is not merely assigned but actively exercised—are not the same thing; a case can complete most of the roadmap's items while still leaving the specific champion-integration item unresolved. Anaheim's own account, that security is now discussed regularly in strategic meetings but that documentation and testing ownership remains unresolved, is consistent with this reading: broad organizational awareness had advanced without a correspondingly settled owner for the day-to-day activity.

Delivery differed across cases. Reporting used tools the teams already had (messaging groups at Etafilia and Pilar, a team chat platform at Anaheim), and security testing relied on low-cost means: AI-assisted testing at Etafilia, and a trial version of an open-source static analysis tool with an AI assistant at Pilar. Items still open at the end were knowledge sharing among developers (X4_P3) in three cases, a written security checklist (X5_P2) and organizational readiness for regulation (X3_P3), where no one could focus on written policies, at Etafilia, and early consideration of security in the SDLC (X2_P2) at Pilar. No documents or operational records were collected; all statements in this section are the informants' own reports.

3.5 Discussion: Pilot evidence, source model, and prior literature

The pilot cannot re-test the mediation model, but the qualitative accounts can be read against it. Where the champion role was exercised in practice, leadership attention took the form of checking completed features and monitoring or reviewing security activity (Etafilia, Kunci, Pilar), a fixed weekly security discussion (Pilar), and passing findings directly to developers (Pilar); that is, leadership worked through testing and remediation routines (X5) and not as a stand-alone activity. This pattern is consistent with the indirect path from security leadership to adoption effectiveness estimated in the source model. It is offered as methodological triangulation [27] and not as statistical confirmation, and because the same informants supplied scores and accounts, it cannot rule out shared perception bias.

The results also bear on the main caution in the security-champion literature. Champions appointed without organizational support tend not to produce the intended change [17], and the role needs continued maintenance after appointment [18]. Three of the four cases avoided this failure mode by tying the champion's activity to existing routines, such as per-feature checks and a weekly review, in line with the view that champions are effective when their influence runs through established organizational routines [19]. The partial result at Anaheim shows the same risk: the role was assigned, yet ownership of testing and documentation remained open.

The staged logic of the roadmap resembles phased adoption reported for ISO/IEC 27001 in small organizations, where controls are introduced incrementally, in order of risk and readiness, and not in one step [24]. Progress in such programs has been tracked by combining a maturity index with staff interviews [25], a mixed quantitative and qualitative design similar to the one used here, and a prioritized, sequenced set of controls is generally considered more realistic for small and medium-sized enterprises than attempting full compliance directly [26]. The present results extend this logic to SSDL in startups, where field evidence on an empirically derived roadmap has been scarce. They show that staged, right-sized governance adoption was feasible in the four cases studied; they do not show that it is better than other sequences, which this design cannot test.

3.6 Limitations

Security culture (X4) was assessed only through two checklist items, proactive reporting and knowledge sharing, which were done in five of eight case-items at the end of the pilot (knowledge sharing in one of four cases). Anaheim's account that security is now discussed regularly in strategic meetings is a single, informal signal that culture may be shifting, and it does not show that X4 develops on a fixed timetable. Direct measurement of X4 over a longer window is left for future work.

The evidence is bounded in several further ways. The four cases were recruited purposively through one regional business association (HIPMI West Java), with one informant per organization, so the results describe these organizations and should not be generalized to the wider startup population. The informants who implemented the roadmap also supplied the pre- and post-implementation scores, the checklist, and the qualitative accounts; no documents or operational records, such as appointment records, review logs, or scan reports, were collected. The data therefore capture perceived change and cannot separate it from actual change in secure development practice, and agreement among the three self-reported sources is not independent corroboration. Social-desirability and consistency bias are possible, although the researcher's involvement was limited to the briefing and to answering questions. Post-implementation scores clustered near the scale maximum (4.4–4.9), which limits sensitivity to further change. The nine-week window is short relative to the time organizational routines need to stabilize, so sustained adoption is not addressed. There was no comparison group, so maturation, seasonal business cycles, and concurrent organizational changes cannot be ruled out. These limitations are consistent with the study's positioning as a naturalistic, ex post pilot evaluation [12] and define the scope within which the findings should be read.

4. CONCLUSIONS

This study evaluated a three-phase security governance roadmap in a naturalistic pilot of four software startups. All four cases reported higher SSDL Adoption Effectiveness after nine weeks (mean increase 1.83; 95% CI 0.77–2.88; Cohen's $d_z = 2.74$); the increase appeared in all five effectiveness indicators, and three of the four startups fully institutionalized a security champion role by tying its activities to routine practice.

These results are preliminary and describe the informants' perceived change. They indicate that the roadmap can be carried out by resource-constrained startups with modest

means, and they provide process-level context for the mediation mechanism estimated in the source model without testing it. For practitioners, the cases support sequencing governance effort (awareness and compliance first, then role formation, then routine practice) and giving security champions named activities inside existing routines rather than a title alone. For research, the study shows that a small key-informant, multi-case pilot can generate implementation evidence for governance artifacts where large samples are hard to obtain.

Given four cases, one self-reporting informant per case, a short window, and no comparison group, the findings should be read as pilot-stage field evidence. Future research should use a larger sample, a longer follow-up, several informants per organization, documentary evidence, and a comparison group, and should apply the complete six-factor roadmap, including security leadership (X6), to an expanded sample.

ACKNOWLEDGMENT

The authors thank the participating software startups and their key informants, recruited through the West Java network of HIPMI, for applying the roadmap and sharing their assessments.

DECLARATION ON THE USE OF GENERATIVE AI AND AI-ASSISTED TECHNOLOGIES

Generative AI tools were used for language refinement during manuscript preparation; all scientific content and conclusions are the authors' own.

REFERENCES

[1] Ferdiansyah, D., Isnanto, R.R., Suseno, J.E. (2023). Organizational indicators on startup software for implementing secure software development lifecycle (SSDL): A systematic literature review. AIP Conference Proceedings, 2683: 050010. https://doi.org/10.1063/5.0125388

[2] Ferdiansyah, D., Isnanto, R.R., Suseno, J.E. (2023). Strategy indicators for secure software development lifecycle in software startups based on information security governance. Journal of Internet Services and Information Security, 13(4): 104-113. https://doi.org/10.58346/JISIS.2023.I4.007

[3] Ferdiansyah, D., Isnanto, R.R., Suseno, J.E. (2026). A strategic governance model for enhancing secure software development in startups: Evidence from Indonesia. KSII Transactions on Internet and Information Systems, 20(8): 4304-4326. https://doi.org/10.3837/tiis.2026.08.018

[4] Daraojimba, A.I., Hamza, O., Collins, A., Onoja, J.P., Eweja, A., Chibunna, U.B. (2025). Creating a scalable model for integrating cybersecurity best practices in early-stage tech startups. International Journal of Scientific Research in Science Engineering and Technology, 12(2): 407-434. https://doi.org/10.32628/IJSRSET25122149

[5] Kempe, E., Massey, A.K. (2021). Regulatory and security standard compliance throughout the software development lifecycle. In Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS), Kauai, Hawaii, USA, pp. 2026-2035. https://doi.org/10.24251/HICSS.2021.248

[6] Otieno, M., Odera, D., Ounza, J.E. (2023). Theory and practice in secure software development lifecycle: A comprehensive survey. World Journal of Advanced Research and Reviews, 18(3): 53-78. https://doi.org/10.30574/wjarr.2023.18.3.0944

[7] Dodson, D., Souppaya, M., Scarfone, K. (2020). Mitigating the risk of software vulnerabilities by adopting a secure software development framework (SSDF). NIST Cybersecurity White Paper, 1-24. https://doi.org/10.6028/NIST.CSWP.04232020

[8] Cheenepalli, J., Hastings, J.D., Ahmed, K.M., Fenner, C. (2025). Advancing DevSecOps in SMEs: Challenges and best practices for secure CI/CD pipelines. In 2025 13th International Symposium on Digital Forensics and Security (ISDFS), Boston, MA, USA, pp. 1-6. https://doi.org/10.1109/ISDFS65363.2025.11011960

[9] Mohammed, K.I., Shanmugam, B., El-Den, J. (2025). Evolution of DevSecOps and its influence on application security: A systematic literature review. Technologies, 13(12): 548. https://doi.org/10.3390/technologies13120548

[10] Naidoo, R., Moller, N. (2022). Building software applications securely with DevSecOps: A socio-technical perspective. Proceedings of the European Conference on Cyber Warfare and Security (ECCWS), 21(1): 198-205. https://doi.org/10.34190/eccws.21.1.295

[11] Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3): 45-77. https://doi.org/10.2753/MIS0742-1222240302

[12] Venable, J., Pries-Heje, J., Baskerville, R. (2016). FEDS: A framework for evaluation in design science research. European Journal of Information Systems, 25(1): 77-89. https://doi.org/10.1057/ejis.2014.36

[13] Kumar, N., Stern, L.W., Anderson, J.C. (1993). Conducting interorganizational research using key informants. Academy of Management Journal, 36(6): 1633-1651. https://doi.org/10.5465/256824

[14] Aalvik, H., Nguyen-Duc, A., Cruzes, D.S., Iovan, M. (2023). Establishing a security champion in agile software teams: A systematic literature review. In Advances in Information and Communication, Springer, Cham, pp. 796-810. https://doi.org/10.1007/978-3-031-28073-3_53

[15] Haney, J., Lutters, W., Jacobs, J. (2021). Cybersecurity advocates: Force multipliers in security behavior change. IEEE Security & Privacy, 19(4): 54-59. https://doi.org/10.1109/MSEC.2021.3077405

[16] Weir, C., Becker, I., Blair, L. (2021). A passion for security: Intervening to help software developers. In 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP), Madrid, ES, pp. 21-30. https://doi.org/10.1109/ICSE-SEIP52600.2021.00011

[17] Gutfleisch, M., Schöps, M., Horstmann, S.A., Wichmann, D., Sasse, M.A. (2023). Security champions without support: Results from a case study with OWASP SAMM in a large-scale e-commerce enterprise. In Proceedings of the 2023 European Symposium on Usable Security (EuroUSEC '23), New York, NY, USA,

pp. 260-276. https://doi.org/10.1145/3617072.3617115
[18] Jaatun, M.G., Cruzes, D.S. (2021). Care and feeding of your security champion. In 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, pp. 63-69. https://doi.org/10.1109/CyberSA52016.2021.9478254
[19] Howell, J.M. (2005). The right stuff: Identifying and developing effective champions of innovation. Academy of Management Perspectives, 19(2): 108-119. https://doi.org/10.5465/ame.2005.16965104
[20] Larios-Vargas, E., Elazhary, O., Yousefi, S., Lowlind, D., Vliek, M.L.W., Storey, M.A. (2023). DASP: A framework for driving the adoption of software security practices. IEEE Transactions on Software Engineering, 49(4): 2892-2919. https://doi.org/10.1109/TSE.2023.3235684
[21] Abdulhassan, A.A., Lafta, A.Y., Jaber, A.S., Kareem, M.I. (2026). Network-centric security awareness in software development: Integrating vulnerability patterns, developer practices, and organizational controls. International Journal of Safety and Security Engineering, 16(2): 327-333. https://doi.org/10.18280/ijsse.160207
[22] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98: 102003. https://doi.org/10.1016/j.cose.2020.102003
[23] Uchendu, B., Nurse, J.R.C., Bada, M., Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109: 102387. https://doi.org/10.1016/j.cose.2021.102387
[24] Kitsios, F., Chatzidimitriou, E., Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector. Sustainability, 15(7): 5828. https://doi.org/10.3390/su15075828
[25] Jevelin, J., Faza, A. (2023). Evaluation the information security management system: A path towards ISO 27001 certification. Journal of Information Systems and Informatics, 5(4): 1240-1256. https://doi.org/10.51519/journalisi.v5i4.572
[26] Mera-Amores, F., Roa, H.N. (2024). Enhancing information security management in small and medium enterprises (SMEs) through ISO 27001 compliance. In Advances in Information and Communication, Springer, Cham, pp. 197-207. https://doi.org/10.1007/978-3-031-53963-3_14
[27] Venkatesh, V., Brown, S.A., Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. MIS Quarterly, 37(1): 21-54. https://doi.org/10.25300/MISQ/2013/37.1.02
[28] Funder, D.C., Ozer, D.J. (2019). Evaluating effect size in psychological research: Sense and nonsense. Advances in Methods and Practices in Psychological Science, 2(2): 156-168. https://doi.org/10.1177/2515245919847202
[29] Runeson, P., Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. Empirical Software Engineering, 14(2): 131-164. https://doi.org/10.1007/s10664-008-9102-8

APPENDIX

Roadmap Implementation Checklist

The 17 checklist items are the indicators retained for X1–X5 in the final source model. Each item was answered "done" or "not yet" by the key informant of each startup at baseline and at the end of the pilot. Phase: roadmap phase the item belongs to (E = emergent outcome). Counts give the number of startups (of four) reporting the item as done. Table A2 gives the scores underlying Table 3 and Figure 2.

Table A1. Checklist items by roadmap phase

Code	Item (indicator)	Phase	Pre (n/4)	Post (n/4)
X1_P1	Understanding of security risk	1	4	4
X1_P2	Understanding of SDLC and risk points	1	4	4
X1_P3	Priority in strategic decisions	1	2	4
X1_P4	Use of security information	1	2	4
X1_P5	Communication with technical team	1	2	4
X2_P2	Security from the start of SDLC	2	0	3
X2_P3	Clarity of security roles	2	1	4
X2_P4	Management support for security	2	1	4
X2_P5	Tools and time for security	2	1	4
X3_P1	Understanding of standards	1	3	4
X3_P2	Monitoring of regulations	1	1	4
X3_P3	Organizational readiness for regulation	1	1	3
X4_P1	Proactive reporting	E	1	4
X4_P3	Knowledge sharing	E	0	1
X5_P1	Routine security testing	3	1	4
X5_P2	Secure coding standards	3	2	3
X5_P3	Rapid remediation	3	2	4

Table A2. Y indicator scores by case (pre/post)

Code	Etafilia	Kunci	Pilar	Anaheim
Y_P1	2.0 / 5.0	4.0 / 5.0	3.0 / 4.5	3.0 / 5.0
Y_P2	2.5 / 5.0	3.5 / 5.0	2.5 / 5.0	2.5 / 4.0
Y_P3	2.0 / 4.5	3.5 / 5.0	2.5 / 5.0	3.0 / 4.5
Y_P4	2.5 / 4.0	4.0 / 4.5	3.0 / 5.0	3.0 / 3.5
Y_P5	2.0 / 5.0	4.0 / 4.5	2.5 / 5.0	2.5 / 5.0
Y	2.2 / 4.7	3.8 / 4.8	2.7 / 4.9	2.8 / 4.4

Each indicator score is the mean of two items on the 1–5 scale; Y is the mean of the five indicators. The scores are the basis of Table 3 and Figure 2.